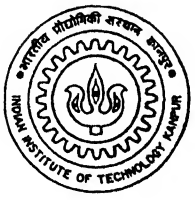
Augmentation and Optimizations of AODV

A Thesis Submitted
in Partial Fulfillment of the Requirements
for the Degree of
Master of Technology

by

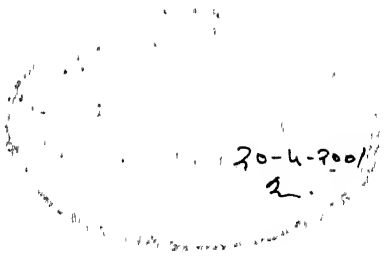
Shailendra Tripathi



to the

Department of Computer Science & Engineering
Indian Institute of Technology, Kanpur

April, 2001



Certificate

This is to certify that the work contained in the thesis entitled "*Augmentation and Optimizations of AODV*", by *Shailendra Tripathi*, has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

April, 2001

20/4/2001

(Dr R K. Ghosh)
Department of Computer Science & Engineering,
Indian Institute of Technology,
Kanpur.

Acknowledgments

First of all, I would like to thank my thesis supervisor Dr R.K. Ghosh for his constant support and guidance throughout the course of my thesis work His sincerity, thoroughness and perseverance has been a constant source of inspiration to me. I shall remain grateful to him for the great interest and devotion he has shown during the course of the thesis.

My friends have always been a great source of inspiration It is their support and critical evaluation which has led me to have a chance to express my gratitude towards them. My friends in BE'95 and MTech '99 have been very good company throughout in my prime part of my life and I have enjoyed the long and enriching discussions I have had with them on matters, technical and mundane.

I would like dedicate my thesis to my uncle, whose sudden demise has left us shattered. He still remains my guide and ideal of my social life Finally, I would like to thank my parents and my family for their constant support, encouragement and patience with me.

Abstract

Mobile Ad Hoc Networks (MANETs) are mobile, multihop, and wireless networks, which are bandwidth constrained, energy constrained, resources constrained, autonomous, and self operating systems with dynamic topologies The aforementioned constraints make the routing between communicating nodes in MANETs very difficult. Numerous solutions have been proposed, but none of these is able to capture the entire spectrum of diversity typically found in wireless networks Instead, the each solution attempts to handle only a subset of the complete problem space.

A routing protocol, Ad Hoc On Demand Distance Vector (AODV), is one of the protocols designed for MANETs that addresses a number of important performance related issues. In this thesis, the protocol has been further augmented and a number of optimizations are included to improve the performances. The first optimization incorporates the utilization of location information for establishing a route between a source and a destination. The results show that in moderate to low mobilities, location information can improve the performance significantly. A source routing scheme is designed which takes the advantages of the cached path as it is employed in DSR [John96]. A new approach has been proposed for taking the advantages of possible local route repairs. Finally, a scheme that provides alternative paths, without adding large extra overhead, has been designed. An idea has been also presented to indicate how this scheme can be used to provide QoS support with AODV.

The proposed protocols are simulated with *ns-2* [Fall00], a widely available experimental network simulator The *ns-2* core component is implemented in C++ and the interfacing is provided through Otcl/Tcl/Tk.

Contents

Acknowledgments iii

Abstract iv

1 Introduction 1

1.1 Emerging Internet 1

1.2 Mobile Ad Hoc Networks 4

1.3 Characteristics of MANETs 5

1.4 Why Mobile Ad Hoc Networks 7

1.5 A Perspective on Applications of MANETs 8

1.6 Hurdles of Mobile Ad Hoc Networks 9

2 Routing in Mobile Ad Hoc Networks 11

2.1 Routing Problem in Networks 11

2.2 Why Routing is Important in MANETs 12

2.3 MANET Routing Protocol Design Issues and Classification 13

2.3.1 Distance Vector Algorithms 15

2.3.2 Link State Algorithms 16

2.4 MANET Routing Protocol Performance Issues 20

3 Ad Hoc Routing Protocols 23

3.1 Destination Sequenced Distance-Vector Routing 23

3.2 Clusterhead Gateway Switch Routing Protocol 24

3.3 Wireless Routing Protocol 25

3 4 Global State Routing 26
3 5 Fisheye State Routing . . 27
3 6 Optimized Link State Algorithm . . 27
3 7 Hierarchical State Routing . . . 28
3 8 Landmark Routing Protocol 29
3 9 Dynamic Source Routing 30
3 10 Ad Hoc On Demand Distance Vector Protocol 32
3 11 Temporally Ordered Routing Algorithm . 33
3 12 Associativity Based Routing 34
3.13 Signal Stability Based Adaptive Routing 36
3 14 Zonal Routing Protocol 37
3 15 Core Extraction Distributed Ad Hoc Routing Protocol 38
3.16 Cluster Based Routing Protocol 38
3.17 Distributed Dynamic Routing Algorithm 39
3 18 Mobile Mesh Protocols 41

4 Effect of Location Information on AODV **43**
4 1 LODV 43
4 1 1 Description of Protocol 44
4 2 GODV 49
4 3 Simulation Model 50
4 3 1 Connection Pattern and Mobility Models 52
4 3 2 Performance Evaluation Criteria 53
4 4 Performance Evaluation 53
4.5 Summary 62

5 Improvements on AODV **63**
5.1 Effect of the Source Route Cache 63
5.1 1 Protocol Description 65
5.1 2 Simulation Model and Performance Criteria 66
5 1 3 Performance Results 66
5 1 4 Summary 69

5 2 Local Repairs in AODV 69
5 2 1 Description of Protocol 75
5 2 2 Simulation Model 76
5 2 3 Performance Evaluation 76
5 2 4 Summary 79
5 3 Alternate Paths and Quality of Service 81
5 4 Effect of Multiple Replies in AODV 81
5 4.1 Protocol Description 82
5.4.2 Simulation Model 83
5 4 3 Performance Results 84
5 4.4 Summary 87

6 Conclusions and Future Work **92**

Bibiliography **98**

List of Figures

1 1 Fixed Access Networks 2
1 2 Networks with Mobile IP 3
1 3 Future Internet 4

2 1 A path from node i to j 12
2 2 Logical View of the Routing Function 12

4 1 Expected Zone of the node after time at t moving at v 44
4 2 Intermediate node closer to the destination 45
4 3 Destination node obstructed by a building 49
4 4 Packet Delivery Fraction at High Packet Rate 55
4 5 Packet Delivery Fraction at Low Packet Rate 56
4 6 Routing Load at High Packet Rate 58
4 7 Routing Load at Low Packet Rate 59
4 8 Average Delay at High Packet Rate 60
4 9 Average Delay at Low Packet Rate 61

5.1 RREQ Packets Flow for a Destination 64
5.2 Packet Delivery Fraction at High Packet Rate 67
5 3 Packet Delivery Fraction at Low Packet Rate 68
5 4 Average Delay at High Packet Rate 70
5 5 Average Delay at Low Packet Rate 71
5 6 Routing Load at High Packet Rate 72
5 7 Routing Load at Low Packet Rate 73
5 8 Link Failure in a Path 74

5 9 Packet Delivery Fraction in a 1 Packet/Sec Network 77
5 10 Packet Delivery Fraction in a Low Packet Network . . . 78
5 11 Average Delay in a 1 Packet/Sec Network 78
5 12 Average Delay in a Low Packet Network 79
5 13 Routing Load in a 1 Packet/Sec Network 80
5 14 Routing Load in a Low Packet Network 80
5 15 RREQ Packets Flow for a Destination 81
5 16 Packet Delivery Fraction at High Packet Rate 85
5 17 Packet Delivery Fraction at Low Packet Rate 86
5.18 Routing Load at High Packet Rate 88
5 19 Routing Load at Low Packet Rate 89
5 20 Average Delay at High Packet Rate 90
5 21 Average Delay at Low Packet Rate 91

Chapter 1

Introduction

There has been a tremendous growth in the field of networking and communication in the last decade. This growth has spurred new possibilities in these fields One such potential field is of Mobile Ad Hoc Networks (MANETs) This chapter first discusses the emerging shape of the Internet with mobility support and wireless enabled connectivity. It presents a characterization of MANETs The potential advantages of MANETs and a vision of the potential applications of MANETs have been also presented. Finally, the chapter provides a brief and comprehensive study on known constraints in MANETs, their future use, and issues in deployment of MANETs.

1.1 Emerging Internet

The Internet has largely been perceived as set of geographically fixed nodes and links till now. It may well be called a fixed Internet. To access the information sources worldwide, the user has to go to some predefined place and then plug some fixed node (figure 1.1) The fixed nature limits its access away from "home" (where the resources are aggregated to be used). Thus, depriving the facilities to the people "on move". The dependency on the World Wide Web (WWW) has tremendously increased in the second half of the last decade. The obvious advantages of the Internet tend to make people increasingly more dependent on it. This reliance is

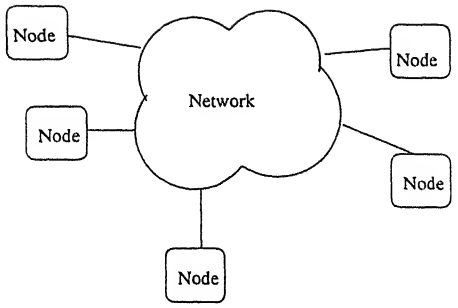


Figure 1 1: Fixed Access Networks

expected to increase with time and as its use becomes progressively more widespread

Traditionally there have been two vistas of information delivery

- Voice, Telephony and Communication
- Data, Networking and Computing

Voice transfer has been considered as synonymous to communication Similarly, data transfer has been perceived as synonymous to networking. The communication has experienced a marked transition from the fixed to mobile in last two decades. The success with mobility in voice communications have a great impact on the research in networks arena to provide mobility in computing With the increasing use of small portable computers (laptops, palmtops), PDAs, hand held devices, digital cellulars and various other wireless devices, providing IP connectivity, the Internet perception is changing swiftly and distinctively.

Mobile IP [Perkins97] enables a node to access the network from anywhere by attaching itself to any point in the network. A mobile IP based network is shown in the figure 1.2. However, mobile IP supported only the portable computing and accessibility of the fixed networks. It still requires an attachment point to the fixed network. Therefore, the mobile IP based network is not suitable for mobile networking and mobile computing, which can be appropriately called as the computing on move.

In recent years, there has been an increasing interest in mobile and wireless networking. The wireless and mobile networks provide the flexibility required for an

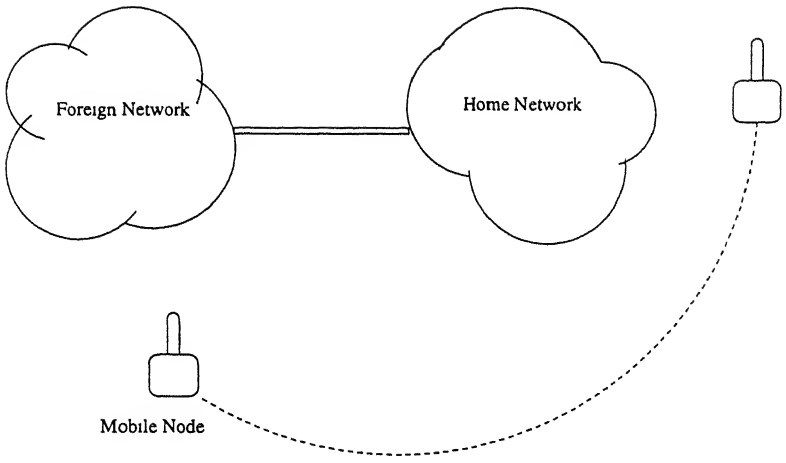


Figure 1 2: Networks with Mobile IP

increasingly mobile work-force. The notion of mobility in computing has introduced a paradigm shift in traditional distributed computing The computation is not only distributed but also needs relocation with mobility of a user Therefore, mobile computing is alternatively referred to as nomadic computing or anywhere and anytime computing

Currently, there is much excitement about the future possibilities realizable by wireless networks. In recent years there has been a tremendous growth in embedded devices. It may found in cellular phones, alarms, automobiles, pagers, palm tops and numerous other devices all around us. In future, it is mooted that these devices will inter-communicate with each other and in a not so distant future will dominate the Internet population

There has been a significant advancement in the field of networking and communications. The communication technologies have begun to support the data transfer. Short Message Service (SMS) provided by the GSM [John97] is just an example of it. The future wireless systems will have inherent support for the data transfer. Similarly, Voice over IP (VoIP) provides the support for the voice communication on the IP based networks [Chris00] The significance of this emerging technology trend, gives a hint of the convergence of the two fields: networking and communication Both areas are abound in systems and standards each dealing with a subset of problems. The present activities in various standard bodies and groups give an

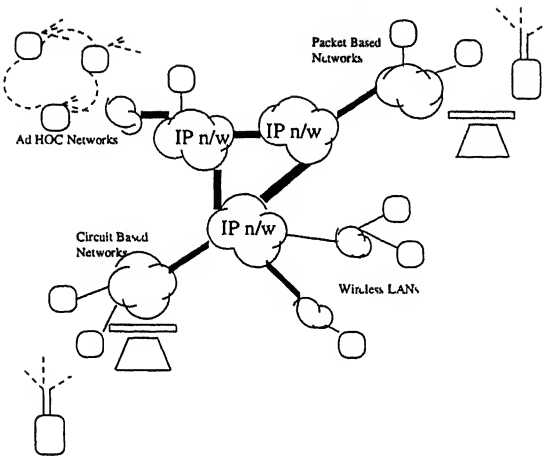


Figure 1.3. Future Internet

ample hint that mobility and Mobile IP will dominate the convergence issues.

There has been a lot interest in making Mobile IP into an integral part of new 3G cellular standards. The number of wireless Internet devices is likely to follow the same exponential growth curve as PC-based Internet devices have followed for some years ago. Third Generation Partnership Projects (3GPP) is trying to achieve the higher data rate. This will result in the increased use of wireless and would require Mobile IP as an integral part of it to access the Internet. The Mobile Wireless Internet Forum of carriers is trying to develop an open Internet based infrastructure for wireless telephones so that it can support all the Internet based services including voice and video, independent of the particular access medium 3GPP2 is trying to do the same (all IP) but heavily influenced by equipment manufacturers than from the operators [IETF47]. Similar trend is also noticeable in IP cellular Networks [Bec00]. Thus, the near future of the Internet will be characterized by mobile IP and everything over IP (figure 1.3). Though overwhelming, still it may not be the end of the road for future possibilities of the convergence of the communication and the networking with mobility support.

1.2 Mobile Ad Hoc Networks

Mobile IP and wireless networks accessing the fixed networks have provided support for the mobility But it is still restrictive in forcing the connectivity at least to the core network It puts impediments on supporting the true mobility in the network In this connection, one area which is getting much attention in last couple of years is Mobile Ad Hoc Networks (MANETs)

Early history of the Mobile Ad Hoc Networking dawns with Mobile Packet Radio Network, a term coined during an early military research in US between late 70's and early 80's. More accurately, it can be called as Mobile, Multihop, Wireless Networking. Ad Hoc Network means a network which is instantiated in an almost improvised way, from generic components, to meet an immediate and specific goal. A MANET consists of mobile platforms (e g., a router with associated hosts and wireless communications devices) which are free to move. The nodes may be located in or on airplanes, ships, trucks, cars, even on persons, or on very small devices, and there may be multiple hosts per router The system may operate in isolation or may have gateways to and interface with a fixed network.

As defined in [rfc2501] a "MANET is an autonomous system of mobile nodes. MANET nodes are equipped with wireless transmitters and receivers using antenna which may be omnidirectional, highly-point-to-point, possibly steerable, etc. At a given point in time, depending on the positions of the nodes and their transmitters and receivers coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or ad hoc network exists among the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters. There is current and future need for dynamic ad hoc networking technology. The emerging field of mobile and nomadic computing, with its current emphasis on mobile IP operation, should gradually broaden and require highly-adaptive mobile networking technology to effectively manage multihop, ad hoc network clusters which can operate autonomously or, more than likely, be attached at some point(s) to the fixed Internet."

1.3 Characteristics of MANETs

Some of the prominent characteristics of MANETs can be summed up as under.

1. *Dynamic Topology* The nodes are mobile and can be connected to the network dynamically and arbitrarily As a result, the network topology will change randomly with time and will be unpredictable It may result in disconnection of the nodes from the rest of the network The network may even be partitioned The topology may consist of both bidirectional and unidirectional links The adjustment of the transmission and reception parameters can have an impact on the topology as well

2 *Resource Constraints·* The ingredients of the mobile network are resource constrained (with respect to a fixed network) The constraint can be in the link itself or in the associated hosts. Some of it include

   - *Bandwidth Constraints* Though there has been a significant increase of bandwidth in wireless networks, it is still very less as compared to the bandwidth available in the fixed networks.

     MANETs often operate in heterogenous wireless environments with significantly varying bandwidth-delay characteristics. Besides, wireless links are affected by many error sources like fading, noise (high), interference conditions and path losses Thus the realizable capacity is much less than a radio's maximum transmission rate. The received signal may be poor, coupled with high error bit rate.

     The less capacity on the links will result in congestion often as a norm than as an exception Since a mobile network is often an extension of the fixed network infrastructure, users, accustomed to the services available in the fixed network, would naturally demand similar services in MANETs. With the increase in multimedia services and collaborative computing, which are highly bandwidth thirsty, the requirements of bandwidth on the links, would be pretty high.

- *Energy Constraints* The mobile nodes rely on the batteries as a source of power. It is invariably inadequate as per the need of nodes Thus, energy efficient designs of the systems and applications add one more dimension of complexity The advancements in battery technologies are also going on, which will provide some relief, but will only be meagre
- *Host Capacity* The smaller embedded devices are set to appear in the mobile wireless networks, accompanied with the limited processing power, the limited storage etc These may have important implications at various levels of design, requiring relocation of computing and traditional client server computing paradigm

3 *Limited Physical Security*: The mobile wireless networks are more prone to physical security threats because the devices may be stolen or the data traffic may have to pass through insecure links. Thus the increased possibility of eavesdropping, spoofing, denial-of-service and various other forms of attacks would require careful attention.

4. *Autonomous and self-operating*: There can be no central entity to manage the nodes All the nodes should take care of the managing itself with respect to the network. The network is infrastructure-less and self-operated

1.4 Why Mobile Ad Hoc Networks

Some of the significant reasons behind the widespread attention of MANETs are:

1 *Ease of Deployment*: Since there is no need for the infrastructure support or support of core administration, MANETs are very easily deployable. The forming of the network requires the participation of nodes which are self organizing and self-operated.

2 *Speed Of Deployment*: MANETS are deployable on-the-fly The reason stems form its characteristics of being autonomous and infrastructure-less.

3 *Cost Of Deployment*: There is no incremental cost for deployment or augmentation as required in fixed networks. However, a greater cost may be associated with the node itself.

4 *Anywhere, Anytime*: A MANET can be formed anywhere at anytime. It is even deployable in certain possible situations where fixed networks deployment will not be easy or, in fact, impossible. The examples include a battalion forming a network in the battlefield.

1.5 A Perspective on Applications of MANETs

The possible applications of MANETs are worth mentioning to appreciate the potentials and the need of MANETs. After all, the critical evaluator is the user who will decide its future.

The military operations are often in very odd places and atypical situations. In such cases, the robustness of the intra-group and inter-group communication can turn out to be the biggest deciding factor. The ease and the speed of deployment which MANETs provides, will be the ideal solution to the communication problem in such tricky situations. It is no coincidence that the development of MANETs have been driven by the demands made by the US military.

The possibilities for commercial success also are huge The recent trend in trade and commerce show an increased reliance on E-mail and Web accesses. As e-commerce gains more acceptance, the reliance will increase more and more. But, the biggest hurdle in user acceptance, is the limitations and the restrictions on electronic form of communication. Nonetheless, recent interest in WAP and its applications are just the precursors of its possible usages. With the support for increased data transfer rate and technological advances in wireless networks, multimedia applications and collaborative computing will become routine affair. The embedded devices of unimaginable future use would be made possible with mobile networks and wireless technology.

Some of the possible future scenarios are mentioned below:

- *Group Communications*: Military applications are just one of the possible uses

of group communications. In any impromptu conferencing, MANETs comes handy. In such situations, MANETs can be created at hand for instant communication. It may be an alternative for communication when infrastructure is damaged due to natural or man made disasters.

- *Personal communications.* Personal Area Networking centers around a user and his equipment. The user may have devices in belts, purses, buttons, glasses, lockets, hand or even pockets All these devices are very close to the person and form a personal area network. These devices may need to communicate which only MANETs can provide In short, MANETs can provide a *personalized infosphere.*

- *Embedded Devices Applications and Home Computing*: Not distant is the future when TV sets, Refrigerators, ACs, Coolers, Burglar Alarms will turn "intelligent". These devices may perform many more tasks not yet completely thought of They may require communication among themselves. For example a thermometer triggering the ACs when temperature goes up, and a press sensor or door sensor signalling burglar alarms.

These are just a few examples its possible usages. As its usage grows, a vast range of applications may emerge not even thought as of today.

1.6 Hurdles of Mobile Ad Hoc Networks

There are many factors which may effectively put dampers to the success of MANETs. These are largely technical than commercial.

- *Performance*: Bandwidth available in wireless networks will continue to be less than their fixed counterparts.

- *Standards* · There has been large proliferation of the available wireless technologies and base standards. Each of them focus on some small area of the whole problem space. This diverse nature provides a huge space for the multiple solutions In addition, there is no common consensus as to how interactions

between standards will take place. Business factors may play their roles as well. Similar is the case with the routing protocols for MANETs. Various solutions have been proposed targeting subproblems of the whole problem space Even then, the transport layer and the application layer decisions may decide the growth of it

- *Security* The vulnerability to security threats may take long to gain users' confidence There may be the need of a focused research for building users' confidence without sacrificing the bandwidth and, hence, the performance.

- *Social Factors* Finally, the users interest and attitude can also play a major role in deciding its future It is assumed that all the users will equally take part in the networking. How malicious users or non-cooperating users should be managed? How to ensure that a node will not power down when it is not supposed to do so? Similarly, it will also depend upon how they will perceive it User education and adaptation according to its behavior can be a deciding factor of the future of the MANETs.

Thus despite having the potential to grow, it is still not clear whether or not it will succeed to full extent or even if it succeeds, what will be its final shape

Chapter 2

Routing in Mobile Ad Hoc Networks

Routing plays an important role in networks The routing decisions in MANETs face considerable challenge due to the constraints and characteristics of MANETs as explained in the previous chapter. This chapter presents an idea about the importance of routing in MANETs. Various design issues pertaining to MANETs have been discussed, and classifications of the existing approaches have been presented. Finally, the various criteria and the parameters for the evaluation of performance of the routing protocol have been addressed.

2.1 Routing Problem in Networks

A network can be viewed as undirected graph G = (V, E), where V is the set of |V| nodes and E is the set of |E| undirected links connecting nodes in V The nodes are the end-points of the networks and the intermediate routers The characteristics of the links may vary depending upon the network, from being wired where it represents the physical link or being wireless where it is logical. The links can be best viewed to represent the end-points of the link which are able to communicate with each other. These links may be associated with weights which may represent bandwidth, latency or any other parameters The routing problem is to find a directed acyclic graph with the only sink at the destination and source at the origin for two communicating pairs (source, destination). A route to the destination j from source i is shown in

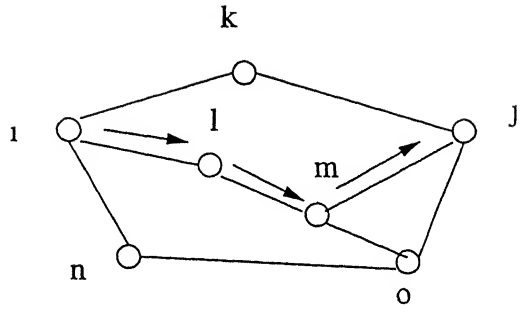


Figure 2.1 A path from node i to j

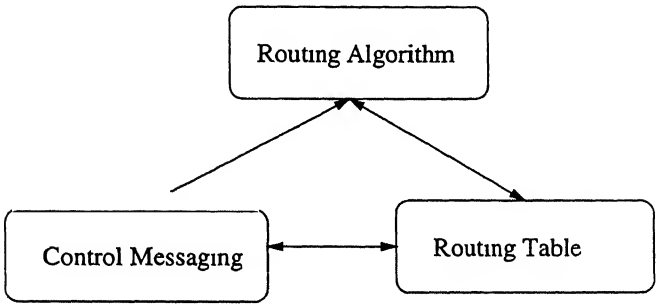


Figure 2.2: Logical View of the Routing Function

figure 2.1

The routing is the network layer function which provides the path between two end-points for communication between them. The key components in it are routing algorithm and control messaging. The routing function can be viewed logically as shown in the figure 2.2

2.2 Why Routing is Important in MANETs

An improved mobile routing capability at the networks layer can provide benefits similar to the original intention of the Internet. That is, an inter-operable inter-networking capability over a heterogenous networking infrastructure But as characterized in the previous chapter, MANETs do not fit in the fixed networks domain Thus, the routing schemes applicable for the fixed networks do not work well in MANETs An IP-like routing in a MANET can provide a real benefit of network

layer consistency. The relegation thus achieved will provide the platform for independent development of physical-layer technologies and MAC sublayer technologies. As new physical-layer or MAC layer technologies are developed, it can be seamlessly added at lower layers without any change in upper layers. Similarly, older technologies can be phased out as well.

That is why to solve the routing problem in MANETs, the earliest approach was that of "Mobile IP". In Mobile IP networks, a mobile host which moves to the foreign network informs the home agent about its new location. The home agent intercepts and forwards the packets to the new location. Thus the basic solution of the routing problem remains intact, i.e., hop-by-hop routing still relies upon the pre-existing routing protocols of the fixed networks. However, Mobile IP requires address management and enhancements in protocol interoperability. Whereas MANET is autonomous and consists of only mobile nodes where everything is mobile. Thus, the topology of the network changes very rapidly. Since there is no such core network as in case of fixed networks or in mobile IP based networks, there is the need to design different solutions to the routing problem in MANETs.

2.3 MANET Routing Protocol Design Issues and Classification

Since the advent of packet radio networks of DARPA, the earliest history of mobile ad hoc networks, a large number of protocols have been developed for the Mobile Ad Hoc Networks. Such networks have different characteristics and requirements as mentioned in section 1.3. The routing protocol should fulfill those requirements and characteristics. The protocols presented often try to solve a subset of the whole problem-set due to the inherent diversity of characteristics of the wireless networks. No routing protocol seems to satisfy the requirements in all the cases. This is largely attributed to the varying requirements and different capabilities in different situations. They differ in performance and usability depending upon the nature of the mobility pattern, nodes characteristics, the systems used, etc.

The routing problem has been well researched in fixed networks. The basic

approach to the routing problem remains same in MANETs The desirable characteristics of a solution include detection and adaptation to the network topology, scalability and convergence These are equally valid for MANETs. However, there is a big difference in dynamicity between fixed network and MANETs. In fixed network, static nature is inherent and dynamicity occurs less frequently While MANETs are inherently, and always, dynamic

As shown in figure 2.2, the routing function consists of three logical components, namely (*i*) routing algorithm, (*ii*) control messaging and (*iii*) routing data The routing algorithm is an abstract scheme to determine how the routing can be achieved The realization of the routing scheme requires some form of control messaging It implies how the control messaging is done, what are the messages, and types It is linked to the routing algorithm as well in its decision Routing tables component creates and maintains the data tables for example topology map, distance vector or routing table

The characteristics of the MANETs (section 1 3) put a number of constraints on all the three components

- The mobility affects the routing algorithms.
- The bandwidth constraint affects the control messaging. and
- The resource constraints affect the routing data choices

Numerous routing protocols have been proposed for MANETs. Each of them try to solve some of the problems associated with these logical components. All algorithms use some form of flooding to achieve the construction of an initial routing data

Depending on the way routing update is carried out, the protocols can be put into two categories.

1 *Flooding Based Algorithms*: These schemes use flooding of routing updates in the network In case of wireless networks, flooding levies an extra overhead Most of the routing protocols are based on this method, like AODV, DSR, GSR etc.

2. *Link Reversal Algorithms.* These algorithms aim to save the bandwidth. Such algorithms are based on constructing DAGs sinked only at each destination Any link breakage results in link reversal algorithm to be used at the site of the link failure to re-establish the path. It tries to localize the effect It gives many alternate paths to the destination. So it not only saves the bandwidth in updates, but also provides alternate paths in case of path failures But it requires some mechanism to detect the link failure One way can be to use the periodic Hello messages, which will incur extra overhead to inform the nodes about the links status. Also the potential disadvantage of this algorithm is that it may not terminate in case of partitioned networks. An example of this method is TORA

2.3.1 Distance Vector Algorithms

Routing by "rumor" is an appropriate phrase to describe the functioning of distance vector based algorithms. All the nodes maintain a table per node in the network containing vector (direction, nexthop) and distance (cost, hop count) information This information is whispered to the neighboring nodes. The receiving nodes update the table for each node based on the "estimates" of the neighbors Only the next hop information is available. No idea of the complete path is known to the node. The example protocols include DSDV, CGSR, GSR. There are many issues involved in it. Some of these are:

1 As it maintains the routing database is maintained for each node in the network, the size becomes very large. Though it is sent only to the neighbors, the MTU (maximum transfer unit) of the network may require more than one network packet. Also the size of the table at the node may affect the resource poor mobile hosts.

2. It suffers from slow convergence The triggered updates to overcome slow convergence may be very costly in the wireless networks. If the changes in the topology are large, flooding of routing packets may occur. Another significant problem in it is "count-to-infinity"

3. Forwarding loops may occur in it due to slow convergence problem

4. It is not scalable due to increase in size of packets with increase in nodes in the network It requires frequent, periodic updates

5. The slow convergence often results in poor robustness as finding multiple paths is not easy

The loop formation can be avoided by associating a destination sequence number ith each route update (DSDV, AODV) and selecting the freshest packet Another pproach is to use the predecessor node information to check the problem (WRP). o solve the large routing update packets, frequent incremental updates are propa- ated and dumping of full routing information is carried out less frequently (DSDV). owever, it requires extra memory and computation. Besides, incremental updates elp only in low mobility.

.3.2 Link State Algorithms

n link state algorithms every node "senses" the status of its direct neighbors, and his link state is then flooded to the whole network. Each node then has the exact subject to time constraints) status of the network and is able to build the complete ietwork topology. From the network topology, every node calculates the shortest ath to the destinations. It can have multiple paths. The example protocols include FSR and OLSR. However, there are several other issues:

1. As the links have severe bandwidth constraints, the flooding of the data packets will affect the bandwidth availability for more useful communication In case of high mobility, the links will often change and, hence, the flooding of control packets occur frequently.

2. A link state algorithm is complex and more compute and as well as memory intensive. In a wireless network all the resources are poor

3. It requires sensing of the links to neighbors very frequently, which puts an extra overhead

Not all the nodes in the network do communicate at all time. Since there is the shortage of the resources at the nodes, one reasonable idea could be to maintain only the routing data for the nodes which are participating in the network Based on this idea, protocols can be classified under three different categories

- *Reactive Schemes* This type of routing protocols find routes only when desired by the source nodes, i.e , only when a source wants to communicate with a destination, a route is established. When the source attempts to send a message to the destination, it initiates route discovery for the destination if it does not already have a route. The route discovery either yields a path or terminates, if no route for the destination exists The path to the destination is maintained throughout the communication and may be deleted either when the route changes or there is no need for it. The latency is higher in such schemes because the path is discovered only when it is required, during which the packets wait in queue. The example protocols are AODV, DSR, TORA, ABR, SSR, CBR, etc.

- *Proactive Schemes*: Such routing protocols try to maintain the paths to all destinations through their route maintenance procedure It maintains some tables having the route information. The route information is propagated across the network when some route changes/link failures occur This way the nodes maintain up-to-date information about other nodes. Though, such schemes have less latency, but may have high routing overhead. Keeping in view the constrained availability of the bandwidth, power and other characteristics of the mobile networks such schemes may be costly. The example protocols are DSDV, GSR, WRP, HSR, CGSR, FSR, OLSR, LANMAR, etc.

- *Hybrid Schemes*: Such protocols may be well thought as exhibiting a mix of the reactive and proactive natures. The example of this protocols are ZRP, DDR and CEDAR etc.

All the protocols attempt to reduce the control messages thrust into the network for providing connectivity. Many protocols for MANETs do not take the advantage of

the "aggregation" of the network in the form of subnets. The scalability problem is, thus, hindered due to the large control messaging. However, the basic solution to reduce the overhead, which is to decompose the whole network into groups, can help here as well That is why a large class of protocols try to create an hierarchy to reduce the messaging in the network. However, the techniques to do so vary considerably in protocols Even a two level hierarchy reduces the messaging overhead. CGSR, LANMAR, and CBRP use two level hierarchy. HSR uses multilevel hierarchy Some scheme like ZRP, FSR and MMRP employ an implicit hierarchy creation method. ZRP creates zones with the radius of some hop around each node The flooding of the network is controlled by letting the nodes at the periphery of a zone to rebroadcast the control packets. FSR and MMRP implicitly create hierarchy by varying the frequency of the updates at different levels of hop length scopes. The core extraction in CEDAR and the tree-forest structuring of DDR also are examples of implicit hierarchy creation. Another approach is to identify the multipoints which are gateway like nodes joining implicitly created clusters as found in OLSR. Another approach can be is to identify the stable nodes and rely more on them for the messaging to reduce the effect of mobility.

Clearly, none of the protocols is able to satisfy the all the requirements. That is, a number of protocols attempt to incorporate more than one idea For instance, there are protocols which take the advantage of both reactive and proactive nature. The reactive nature often reduces the overhead and proactive nature, reduces the latency. ZRP, CEDAR and DDR work on utilizing this philosophy Significantly distinct approach is taken by LANMAR, which uses linkstate algorithms at group level and distance vector algorithms at *Landmarks* level.

Many other schemes use query localization approach to reduce the flooding of the packets. Some routing protocols seek help of the physical location to reduce the query overhead, if available. Location Aided Routing, and adaptations of this scheme are examples of it. The location information may be obtained from GPS like systems, and can be either proactively or reactively advertised across the network. There may be other criteria for the categorization of the routing protocols. Depending on the intended use protocols may be categorized broadly as follows

- *Unicasting*: Includes all such protocols which are used for end-to-end communication.

- *Multicasting* It includes all such protocols which can be used for one-to-many communication

- *Geocasting* It includes all such protocols which can be used for geographic communication. Geocasting is different from multicasting in the fact that the group defined in the former is based on physical location whereas that in multicasting the destination of a group is purely logical, the nodes may be physically located anywhere

Yet another way to classify routing protocols may be based on the network hierarchies. A network may be.

- *Flat* In this kind of network, all the nodes are on the same level.

- *Hierarchical*: In such kind of networks, nodes are logically or physically on a different level of hierarchy

The type of the deployment of the MANETs influences the design protocols considerably Depending upon the capabilities and roles of the nodes, the protocols proposed may be:

- *Symmetric Network*: Where nodes participating in the network have equal capabilities and responsibilities.

- *Asymmetric Network*: Where nodes participating in the network may have different capabilities like transmission range, processing and storage capacity, battery life etc. The nodes may have different roles as well, like only a set of selected nodes taking part in the routing. Some specific nodes may react differently with respect to routing.

- *Wired cum wireless Network*: In such networks, both wired and wireless type of nodes may co-exist.

There can be other categorization criteria as well

- Whether the protocol uses flooding for data dissemination on route search or uses some form of graph for it
- Whether protocol floods the data or the control packets
- The protocol keeps the security into considerations or not
- Whether the protocol can support the Quality of Service or not
- Whether the protocol takes care of the energy power or not

It can be safely assumed that as much diverse is the wireless networking field so much diverse are the routing protocols for it There does not seem to be a consensus on any protocol, and hence further explorations are still under way

2.4 MANET Routing Protocol Performance Issues

The merit of a routing protocol can be evaluated either through qualitative or quantitative metrics. A set of desirable properties of MANET routing protocols is listed below

- *Distributed operation*: The route computation should be distributed because centralized routing in a dynamic network is not suitable even for fairly small networks
- *Loop-freedom*: Though not mandatory, it is desirable to avoid problems like packets looping in the network for an arbitrary period of time. The TTL value can be used to restrict the packet looping problem.
- *Demand-based operation*. The routing algorithm should adapt to traffic on demand for efficient utilization of network energy and bandwidth resources. Though, an obvious drawback of on demand operation would be increased route discovery delay.

- *Proactive operation*: Sometimes, the additional latency, incurred due to demand based operation, may not be acceptable. So, where the resources and bandwidth availability permit, proactive operation may be preferred

- *Security* A MANET routing protocol is vulnerable to many forms of security attacks if some form of network-layer and link layer security is not in place. Snooping network traffic, replaying transmissions, redirecting routing message, and manipulating packet headers are fairly simple in such networks. While security concerns exist within wired infrastructures, and routing protocols as well, maintaining the physical security of the transmission media is harder in practice with MANETs. Sufficient security will be required to gain the confidence of the users

- *Sleep period operation* For the purpose of energy conservation or some reasons, nodes of a MANET may be forced to remain inactive. During this period nodes may stop transmitting and receiving for arbitrary amount of time A routing protocol should be able to accommodate such sleep periods

- *Unidirectional link support*· Many algorithms typically assume bi-directional links, and thus, are able to work properly on unidirectional links However, unidirectional links can occur in wireless networks.

Following are the set of quantitative metrics which can be used to assess the performance of a routing protocol·

- *End-to-End throughput and delay* Data routing performance can be measured by statistical measures like means, variances or distributions These imply the effectiveness of the routing protocol

- *Route Discovery Time*: This particularly is a concern of on demand routing algorithms.

- *Percentage Out-Of-Delivery*· The measure of performance of connectionless delivery.

- *Efficiency*: Efficiency is the internal performance of its effectiveness. Two different protocols can spend different amounts of overhead, depending upon the internal efficiency Protocol efficiency may or may not directly affect data routing performance If control and data traffic must share the same channel, and the channel's capacity is limited, then excessive control often impacts data routing performance

The internal efficiency of a protocol can be assessed by a few ratios like

1 Average number of data bits transmitted to the data bit delivered This is the bit efficiency of delivering data within the network

2. Average number of control bits transmitted to the data bit delivered This is the bit efficiency of the protocol with respect to control overhead. It should include all the bits in the packets that are not data bits.

3 Average number of control and data packets transmitted to the data delivered: Instead of pure algorithmic efficiency as shown by the bit efficiency, it tries to capture the protocols channel access efficiency, which may be high in contention based link layers.

Chapter 3

Ad Hoc Routing Protocols

This chapter briefly reviews some of the well known existing protocols. Only the main idea behind each design of each protocol has been presented. The details of various optimizations employed in different protocols may be found in respective protocol proposal references cited in the text Many of the protocols are *Work in Progress* and under development by the *manet* working group of *IETF*.

3.1 Destination Sequenced Distance-Vector Routing

Destination Sequenced Distance-Vector Routing (DSDV) [Bhag94] is an adaptation of the classical Bellman Ford Algorithm for finding shortest path in MANETs . It eliminates the loop formation problem associated with the distance vector algorithms using destination sequenced numbers with each update message. Every node keeps routing information for all the nodes of the network The routing table updates are sent periodically and on any change in topology across the network. Since the number of nodes may be large, the update message may be very large exceeding the maximum transfer unit of the network protocol. To alleviate this problem, the routing update may be

- full dump in which the complete topology information is sent or

- incremental change packets in which only changed entries since the last update message, are sent

However, this approach helps when the mobility is relatively low Otherwise, the size of the incremental change packets size may be large again. The routing update messages, tagged with the largest sequence number, are selected by the receiving nodes Since the route update takes a finite time in converging, average settling time is maintained to avoid the possible problems which may occur in the network. Some informations are advertised immediately, for example (i) new node, (ii) route failures and (iii) repaired routes, due to failed link, coming up

The bulk of the complexity in DSDV is in generating and maintaining these routing tables The route update packets are broadcast throughout the network, so every node in the network has a route to every other node. As the number of nodes in the network grows, the size of the routing tables and the bandwidth required to update these also grows. The update is periodic which occurs even if there is no change in the topology. This is the main weakness of DSDV On topology changes, routes become unstable This unstability may be more noticeable with high mobility in the network. To avoid cascading effect of flooding, due to advertisement of unstable routes, DSDV requires a finite amount of route settling time With low mobility and for small size network, it performs well as its latency and the routing overhead will be low. Though it provides one path, but it selects the shortest path based on the hop count metric

3.2 Clusterhead Gateway Switch Routing Protocol

Clusterhead Gateway Switch Routing Protocol (CGSR) [Chi97] is basically DSDV algorithm but instead of flat networks, it assumes hierarchical network. The network is divided into clusters, each having a clusterhead, which communicate with the other clusters through gateways, the nodes common to more than one clusters. By having such arrangement, the authors claim that different channel access schemes, routing and/or bandwidth allocation policies can be employed in different clusters. A distributed algorithm is used to elect the cluster head. Within cluster, the nodes

communicate directly with the nodes For the node in other cluster, the node sends packets to its cluster head which forwards it to the neighbor cluster head through gateway until the destination cluster head is reached Then, it the packets are forwarded to the destination node. Each node maintains the information about all the nodes in its cluster and for all the cluster heads This information is periodically broadcasted in network The rest scheme is similar to the DSDV scheme

The cluster head election, takes significant time, in dynamic network may degrade the performance The election time taken grows with number of times the election is employed To avoid it, least cluster head methods is used, in which the cluster head is not changed until (i) two cluster heads come into the same cluster due to change in network topology or (ii) a node drifts away from all the cluster heads This scheme suffers from the same problems as with DSDV. However, the overhead is reduced due to this clustering. The latency is dependent on the status of the cluster heads, gateways and other nodes. The cluster-head election significant may incur overhead on latency time which depends upon how many times the election occurs.

3.3 Wireless Routing Protocol

Wireless Routing Protocol (WRP) is a proactive distance vector routing protocol [Gerla98] Each node maintains a routing table, a distance vector, a link-cost table, and a message transmission table (MRL table). The Distance table contains the distance metric for each of the destinations through each of its neighbors. The routing table maintains the distance metric, the predecessor and the successor node of each node. The link-cost table maintains the cost to the neighbor and the timing related information since the last error free message has been received.Each entry in the MRL table has sequence number of the update message, a retransmission counter, ack-required flag for each neighbor and list of updates sent in the update message. The MRL records the update messages which must be retransmitted and also the list of neighbors from which acknowledgement about the retransmitted updates are yet to be received. It ensures reliable delivery of updates. A neighbor

node can determine whether it has sent an acknowledgement to a update message through MRL. The update is sent when there is change in the link or the update messages from the neighbors contain the update

The connectivity information is maintained by periodic Hello messages to the neighbors A timeout in wait is considered the link failure. The nodes detect new nodes through Hello messages

As it requires four tables to be maintained, the memory requirements increase with the increasing number of nodes in the network Frequent Hello messages too consume bandwidth and energy However, it is free form the routing loops problem It avoids the "count-to-infinity" problem by enforcing the nodes to check the predecessors of the neighbors. However, in fast changing environment, loop may exist for some time.

3.4 Global State Routing

Global State Routing (GSR) [Chen98] is similar to DSDV scheme, but it uses the link states instead of distance vectors. It maintains a neighbor list, a topology table, a next hop table and a distance table. For each destination, the topology table contains the linkstate information received from the destination along with a sequence number. The distance table contains the shortest distance to the destination.

Based on the link state information it updates the topology table and then computes the routing table. GSR does not floods the link state packets as in linkstate schemes, it maintains a link state table at each node based on the information received form the neighbors. The information is exchanged periodically with the neighbors. The update is selected based on the time stamp of the sequence numbers The routing messages are generated as topology changes.

The size of table does not vary much with increasing number of nodes, in case of high mobility the convergence may take significant amount of time. The route settling time is large for high mobilities. Besides, the update interval is very critical because large periods may degrade the performance.

3.5 Fisheye State Routing

Fisheye State Routing(FSR) [Pei00] is an adaptation of the link state protocol to the mobile environment It is similar to the GSR in the approach that it sends update message to its neighbors only Each link state entry is sequenced to prevent loop formation. It creates an implicit hierarchical routing. The resolution of routing information is a function of the distance from the destination Accurate information about the node is maintained towards the immediate neighborhood, and with increasing distance, less detailed information is maintained. The overhead of the link state update packets is reduced as update is not broadcasted to all the nodes. The routing update message is not event-triggered instead it is periodic only. The sequenced periodic table update resembles the vector exchange in Destination-Sequenced Distance-Vector Routing (DSDV)

Though the scoping, as described above, reduces the overhead as compared with the link state algorithms, the overhead grows with the size of the network. As with the all class of proactive algorithms, even for the non-active nodes, the topology information is maintained. The memory requirements grow with the number of the nodes in the network as it stores information for each node in the network. The protocol is robust with the host-mobility because the link change does not impulse farther nodes very frequently. The scope size selection may be crucial because large scope sizes may result in large overhead. The longer the update interval, the less accurate the routing information However, several features of FSR reduce the routing inaccuracy. For large network size, as the route error is weighted by distance, the sensitivity to network size is largely reduced.

3.6 Optimized Link State Algorithm

Optimized Link State Routing (OLSR) [Jac01] is a link state routing protocol adapted to the MANETs. The novel attribute of OLSR is its ability to track and use multi-point relays (MPRs), the neighbors of a node such that each two hop neighbors of the node is a one-hop neighbor of at least one multipoint relays of the node. The MPRs are selected nodes which forward broadcast messages during the

flooding process. The neighbors which are not in the multi-point relay receive any packet but do not re-transmit it.

This technique reduces the message overhead as compared to pure flooding mechanism where every node retransmits each message In OLSR, information flooded in the network "through" the MPRs is also about the MPRs Thus a second optimization is achieved by minimizing the "contents" of the control messages flooded in the network Hence, as contrary to the classic link state algorithm, only a small subset of links with the neighbor nodes are propagated This information is then used by the OLSR protocol for route calculation.

Though the protocol may perform well in the dense and the large network, it may not perform well in sparse network Its performance will depend upon the multipoint relays. OLSR is well suited for networks, where the traffic is random and sporadic between "several" nodes rather than being almost exclusively between a small set of specific nodes. Its performance is thus topology based and unpredictable Use of MPRs restrict it to work only for bidirectional links. As it requires that each node in the network, sends a message containing the addresses of the neighbors which have selected the node as a MPR, for large networks the overhead may be high. The protocol requires link status sensing. This service is provided by sending/receiving periodic HELLO messages to/from one hop neighbors. It results in extra overhead on the network to maintain the connectivity.

3.7 Hierarchical State Routing

Hierarchical State Routing (HSR) [Iwata99] works on multi-level, clustered and logically partitioned network. A cluster-head is elected similar to other cluster-based algorithms. In HSR, the cluster-heads again organize themselves into clusters, elect a cluster head and so on, to form the hierarchy. The nodes of a physical cluster broadcast their link information to each other. The cluster-head summarizes its cluster's information and sends it to neighboring cluster-heads via gateway as it is in CGSR. These cluster-heads are member of the cluster on a level higher and exchange their link information among that level and so on, up to the highest level.

A node at each level floods to its lower level the information that it obtains after the algorithm has run at that level. So the lower level has a hierarchical topology information Each node is identified by a hierarchical address The hierarchical address may be so assigned that it reflects the clustering order form top to bottom A gateway can be reached from the root via more than one path, so the gateway can have more than one hierarchical address. Thus, the hierarchical address is enough to ensure delivery from anywhere in the network to the host

Further, the nodes are also partitioned into logical subnetworks and each node is assigned a logical address <subnet,host>. Each subnetwork has a location management server (LMS) All the nodes of the subnet register their logical address with the LMS The LMS advertise their hierarchical addresses to the top levels and the information is sent also to all LMS at lower layers. The transport layer sends a packet to the network layer with the logical address of the destination. The network layer finds the hierarchical address of the destination from its LMS and then sends the packet to it. The destination LMS forwards the packet to the destination. Once the source and destination know each others hierarchical addresses, they can bypass the LMS and communicate directly. Since logical/hierarchical address is used for routing, it is adaptable to network changes. The hierarchy, thus, imposed reduces the overhead associated with the link state algorithms and reduces the entries in the routing table.

But it requires the location management servers with up-to-date information about the addresses The failures of a LMS can affect the protocol. Thus, it is dependent upon a central entity. It requires the extra storage and computation to maintain the location database as well.

3.8 Landmark Routing Protocol

It can be well thought as mix of a "scoped" routing protocol like FSR and hierarchical protocol like HSR. The Landmark Routing Protocol (LANMAR) [Hong00] utilizes the concept of "landmarks" for scalable routing in large, mobile ad hoc networks. It relies on the notion of group mobility, i.e., a logical group (for example a team of

coworkers at a convention) moves in a coordinated fashion. The network address of a node is assigned as <Group ID, Host ID>. A landmark is dynamically elected in each group. The route to a landmark is propagated throughout the network using a distance vector mechanisms. Separately, each node in the network uses a "scoped" routing algorithm (e.g , FSR) to learn about route within a given (max number of hops) scope To route a packet to a destination outside its scope, a node will direct the packet to the landmark corresponding to the group ID of such destination.

The main advantage of LANMAR is that the routing table includes only the nodes within the scope and the landmark nodes. Once the packet is within the scope of the landmark, it will typically be routed directly to the destination. The remote groups of nodes are "summarized" by the corresponding landmarks. For the nodes presently not in the range of the group, drifters tables is maintained, which contains the informations of the drifter node. The solution to drifters (i.e., nodes outside of the scope of their landmark) is also handled by LANMAR.

Extra storage, processing and link overhead will be incurred for landmark election and drifter bookkeeping. It may increase overall latency Also the drifters bookkeeping overhead may be large if the number of drifters is high. It scales well in large scalable networks. The landmark information is sent periodically, even if there is no change in the topology and it tracks even the non-active nodes, which are often unused. Besides, the size of the scope is crucial and may affect the performance considerably.

3.9 Dynamic Source Routing

The Dynamic Source Routing Protocol(DSR) [John96] is a source-routed on-demand routing protocol. The DSR protocol allows nodes to dynamically discover a source route. Each data packet carries the complete, ordered list of nodes through which the packet will pass in its header, allowing packet routing to be trivially loop-free and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded. By including the source route in the header of each data packet, other nodes forwarding or overhearing any of these packets may

also easily cache this routing information for future use. The protocol is composed of the two mechanisms, namely "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network

DSR requires no periodic packets of any kind at any level within the network. For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbor detection packets, and does not rely on these functions from any underlying protocols in the network. The network topology changes not affecting routes currently in use are ignored and do not cause reaction from the protocol In response to a single route discovery (as well as through routing information from other overheard packets), a node may learn and cache multiple routes to any destination If the node does not have such a route, then it initiates the route discovery process by broadcasting a route request packet. The route request packet contains the address of the source and the destination, and a unique identification number. Each intermediate node checks whether it knows of a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors.

To limit the number of route requests, the nodes process the route request packet only if it has not already seen the packet and its address is not present in the route record of the packet. A route reply is generated when either the destination or an intermediate node with current information about the destination receives the route request packet. A route request packet reaching such a node already contains, in its route record, the sequence of hops taken from the source to this node. Route reply can be sent by reversing the path only if links are guaranteed to be bi-directional Otherwise, the route discovery is initiated and route reply is piggybacked on it.

When a node encounters a fatal transmission problem at its data link layer, it generates a route error packet. A node receiving a route error packet, removes the associated hop from its route cache. All the routes containing the broken link are truncated at that point. The acknowledgment packets are used to verify the correct operation of the route links. It also includes passive acknowledgments in which a node hears the next hop forwarding the packet along the route. As the reply may

result in reply storm, reply should be delayed for a random period of time.

Packet header size grows with the route length So for the large routes, it may result in a significant overhead Stale caching can adversely affect performance. With passage of time and host mobility, cached routes may become invalid. So a sender may try many cached routes before finding a correct path. The flood of route requests may potentially reach all nodes in the network And at times it may result in broadcast storm problem Care must be taken to avoid collisions between route requests propagated by the neighboring nodes An intermediate node may send route reply using a stale cached route, thus polluting other caches

3.10 Ad Hoc On Demand Distance Vector Protocol

Ad hoc On-demand Distance Vector Routing (AODV) [Royer01] is an improvement of DSDV and DSR protocols. AODV retains the desirable feature of DSR that routes are discovered on demand. The route requests (RREQ) are forwarded in a manner similar to DSR. It reduces the need for the system wide broadcasts by localizing the propagation of change in the network. If the link status does affect the ongoing communication, no broadcast occurs Only when a distant source tries to use path with broken links, nonlocal effect occurs. The nodes using the route with broken links are informed. The routes which are not used are expired and discarded. Thus, it removes the stale and unused routes Like DSDV, it uses the sequence number to avoid the loop formation problem.

However, the routing table construction is different from DSR. During route request traversal, it sets up a reverse path pointing towards the source When the destination replies it replies, the route reply packets travels along the reverse path set-up while route request was forwarded. An intermediate node may also send a RREP packet, provided the intermediate node has more recent path which is determined by the sequence numbers. A new route request for a destination is assigned a higher destination sequence number than the known value. A routing table entry maintaining a reverse path is purged after a timeout interval with timeout long enough to allow RREP to come back in the worst case. A routing table entry

maintaining a forward path is purged if not used for an active route timeout interval. If no data is being sent using a particular routing table entry, the entry will be deleted from the routing table

When a link breaks, all the active neighbors are informed The link failures are propagated using route error messages. When the source receives the RERR, it initiates a new route discovery. The neighbor nodes connectivity must be ensured either using hello message periodically or taking the feedback from the lower layers. The absence of hello messages are used as an indication of link failure In latter, failure to receive several MAC-level acknowledgement may be used as an indication of link failure. Since the route request broadcast may result in broadcast storm problem, source uses expanding ring search method by setting a Time-To-Live (TTL) value TTL specifies the diameter of the subsection of the network in which RREQ is allowed to spread. If the route is not found within the timeout, a new TTL and timeout value is set to search again. This is repeated till a threshold value of the TTL, then TTL is set equal to the network diameter and this process is repeated RREQ_RETRIES times before aborting the process.

A route request results in only one path. The likelihood that an intermediate node will send a route reply when using AODV is not as high as DSR So the routing load in AODV is relatively higher than DSR. Also it uses periodic beaconing from the nodes to maintain the neighbor connectivity which is an overhead associated with it. Memory requirements may be higher in DSR as it maintains more information than the AODV. It is not very much suitable for unidirectional links. A list of precursors is maintained at each node on the path. A precursor is a neighbor of the node which is using the node on at least one of its active paths. It is used to send the RERR packets to the nodes using the link, when link breaks.

3.11 Temporally Ordered Routing Algorithm

Temporally Ordered Routing Algorithm (TORA) [Park97], is neither distance-vector scheme nor link-state based scheme. In fact it employs a partial link reversal algorithm The protocol can simultaneously support both source-initiated, on-demand

routing for some destinations and destination-initiated, proactive routing for other destinations It modifies the partial link reversal method to be able to detect the partitions. It finds multiple routes from a source node to a destination node The main feature of TORA is that the control messages are localized to a very small set of nodes around the region where topological changes occur To achieve this, the nodes maintain routing information about adjacent nodes It also stops non-productive link reversals TORA constructs the DAG having the destination as a only sink This way it results in many routes to the destinations In case of link failures, it reverses the links until the DAG is restored.

TORA maintains state on a per-destination basis. The destination-oriented nature of the routing structure in TORA supports a mix of reactive and proactive routing on a per-destination basis TORA has been designed to work on top of lower layer mechanisms or protocols that provide the following basic services between neighboring routers· link status sensing and neighbor discovery, reliable, in-order control packet delivery and link and network layer address resolution and mapping In TORA there is a potential scope for oscillations to occur, especially when multiple sets of coordinating nodes are concurrently detecting partitions, erasing routes, and building new routes. Because TORA uses inter nodal coordination, its instability problem is similar to the "count-to-infinity" problem in distance-vector routing protocols, except that such oscillations are temporary and route convergence will eventually occur. Any node declares that there is a partition when it receives reflection from all the neighbors. On detecting a partition, it sends route clear message which clears all the directed links in that partition.

3.12 Associativity Based Routing

The Associativity Based Routing (ABR) [Toh97] defines a new metric for routing known as the degree of association stability, which means the connection stability of one node with respect to another node over time and space Only the links that have been stable for some minimum duration are utilized The basic idea is to avoid the unstable links form the route as much as possible All the nodes generate

periodic beacons On each beacon, the nodes update its associativity tables. For every beacon received, the associativity index, with respect to the node from which it received the beacon, is incremented The associativity index is reset when the neighbors of a node or the node itself moves out of the proximity

The route discovery is very much similar to DSR, which includes the association index as well The destination receives many paths among which it can select path based on higher aggregate association stability The node on the reply path are marked valid Depending on the movement of nodes from the paths, in a route reconstruction phase, a partial route discovery, an invalid route erasure, valid route updates, and a new route discovery are done. The route notification (RN) message is used to erase the route entries in the nodes

When the destination moves, the destination's immediate upstream node erases its route. A localized query (LQ) process is initiated to determine if the node is still reachable. If the destination receives the LQ packet, it selects the best partial route and sends replies. Otherwise, the initiating node times out and backtracks to the next upstream node. An RN message is sent to the next upstream node to erase the invalid route and inform the node that it should invoke the LQ process. If the process results in backtracking more than halfway to the source, the LQ process is discontinued, and the source initiates a new broadcast route discovery process. When a discovered route is no longer required, the source node initiates a route delete (RD) broadcast All nodes along the route, delete the route entry from their routing tables. The RD message is propagated by a full broadcast, as opposed to a directed broadcast, because the source node may not be aware of any route node changes that occurred during route reconstructions

On demand nature increases the latency. Periodic beaconing to maintain the association stability index, is an overhead The protocol will work well when the network is relatively stable At very high mobility, the stability criteria may not be satisfied or even if it is satisfied, it may result in, long, and hence, unoptimized paths The long paths may also affect the overall delay

3.13 Signal Stability Based Adaptive Routing

Signal Stability-Based Adaptive Routing protocol (SSR) [Dube97] is an on-demand routing protocol like AODV which selects the routes based on the signal strength between the nodes. The nodes re-broadcast the route requests only when the link is likely to have strong signal stability. Thus, effectively, the routes that have "stronger" connectivity are selected.

The SSR comprises of two cooperative protocols. the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP). The DRP maintains the Signal Stability Table (SST) and Routing Table (RT) The SST stores the signal strength of neighboring nodes obtained by periodic beacons from the link layer of each neighboring node. The signal strength is either recorded as a strong or weak channel All transmissions are received by DRP and processed After updating the appropriate table entries, the DRP passes the packet to the SRP The SRP passes the packet up the stack if it is the intended receiver. If not, it looks up the destination in the RT and forwards the packet. If there is no entry for the destination in the RT, it initiates a route-search process to find a route. The destination replies to the first route-search packet reaching the destination. The DRP reverses the selected route and sends a route-reply message back to the source

The route-search packets reaching the destination must have arrived on stronger signal stability path. If the source times out before receiving a reply then it changes the preference field in the header to indicate that weak channels are acceptable, since these may be the only links over which the packet can be propagated. When a link failure is detected within the network, the intermediate nodes send an error message to the source indicating which channel has failed. The source then sends an erase message to notify all nodes of the broken link and initiates a new route-search process to find a new path to the destination.

It uses two protocols which results in extra overhead in interfacing and cooperation. The on demand nature along with the possibility of not getting the stronger stability path at all, very often results in delays The paths obtained are longer and periodic beaconing results in extra overhead. It results in only one path, and it assumes bi-directional links.

3.14 Zonal Routing Protocol

Zone Routing Protocol (ZRP) [Haas01] is a hybrid protocol which is based on both the reactive and the proactive approaches. It partitions the network implicitly into zones. The zone is defined as all such nearby nodes which can be reached within zone-radius defined in hops from the node It applies proactive strategy inside the zone and reactive strategy outside the local zone. Each node may be potentially located in many zones. All such nodes which are exactly at the zone radius distance are called border nodes. The proactive intra-zone routing protocol (IARP) is an adapted distance-vector algorithm. When a source has no IARP route to a destination, it invokes a reactive inter-zone routing protocol (IERP) which is very similar to DSR.

The source bordercasts a route request to its border nodes, on receiving the request, after consultation of the local zone routing information. If the destination is not in the border node's zone, it adds its ID to the request and re-bordercasts the route request. When the request reaches a border node whose zone includes the destination, it contains a non-strict source route to the destination, i.e , each listed node has a IARP route to the next and previous elements in the source route. This loose source route can be used to accumulate a complete source route, or portions of the route can be cached at intermediate nodes. Route failure is detected proactively, in conjunction with the IARP. Failures may be repaired locally, in which case it may not even be necessary to inform the source node. If necessary, a hop-limited local request can be used to repair the route, or a route error message can be sent to re-initiate the route discovery from the source.

The bordercast is more expensive than the broadcast and flooding used in other reactive protocols because nodes generally have many more border nodes than the neighbors. In addition, each bordercast message has to traverse zone-radius hops to the border which may be unnecessary in many cases. Number of optimizations have been proposed to reduce the overhead. The IARP topology information maintained at each node can help in avoiding the many problems and selective bordercasting. Selective bordercasting is similar to the MPR selection used in OLSR, each node selects a subset of its border nodes that achieves equivalent coverage. However, routes are found very fast within the zone.

3.15 Core Extraction Distributed Ad Hoc Routing Protocol

Core Extraction Distributed Ad hoc Routing (CEDAR) [Sinha99] is a hierarchical protocol which attempts to model the IP routing structure, emphasizing QoS support, by identifying a subset of nodes called core Each node must be adjacent to least one core node and picks one node as leader or dominator The core is determined by periodic messages exchange between each node and its neighbors Each core node maintains a path to the nearby nodes by issuing a limited broadcast.

CEDAR has three components: core extraction, link state propagation and route computation. The core is dynamically extracted by approximating a minimum dominating set using local computation and local state. The core performs route computation on behalf of the nodes which belong to it. The bandwidth availability information is then propagated in the core subgraph. The stable and large bandwidth links are propagated farther in the network than dynamic and less bandwidth links. It uses the link state for propagating the routing information. Each core node knows about local links and nodes which are stable or having high bandwidth When a source wants to send the packet to the destination, it informs its core Then the core node finds the path to the core node of the destination using some DSR like probing. Then core nodes form a path using locally available link state information

The core extraction results in increased overhead Since, the communication is done through nodes having high bandwidth or low delay requirements, the performance of the protocol is dependent upon the relative position of the such nodes in the network. On demand nature may result in increased delay. However, the protocol utilizes the partitioning to reduce the overhead.

3.16 Cluster Based Routing Protocol

Cluster Based Routing Protocol (CBRP) [Tay99] is a hierarchical protocol which partitions the network into clusters like CGSR. However it is different from CGSR because it discovers the paths on demand. It can be used on uni-directional links as

well. Though the clusters are defined by bi-directional links, inter-cluster connectivity can be achieved by a pair of uni-directional links The clusters may be disjoint or overlapping; one node is elected cluster-head. It is source routing protocol like DSR and and uses gateways to achieve inter-cluster communication like CGSR.

Each cluster-head sends the route request to its neighboring clusters by appending its address in the route request packets. Each cluster-head has the exact topology information about its cluster. Finally, when it reaches the destination cluster-head, using gateways, it has a loose-source route to the destination. On reply, it may follow the same path, if still, available or it can follow another path in case of uni-directional links. At each cluster, optimized path may be added on reply, depending upon the current status of the cluster. The packets take the path thus obtained as source route. Similar to DSR, intermediate nodes may generate new routes to take advantage of improved routes or salvage failed routes. Unlike DSR, only cluster-level information may be used for this purpose. nodes do not attempt to cache network-wide topology information. In addition to exchanging neighbor information for cluster formation, nodes must find and inform their cluster-head(s) about the status of gateway nodes. Thus, each cluster-head has knowledge of all clusters with which it has bidirectional connectivity.

Since the route is maintained for the required destinations only, it reduces the overhead considerably. The path obtained us optimized. However, it may have considerable latency. The position of the cluster-head and the gateways, affect the performance of the protocol.

3.17 Distributed Dynamic Routing Algorithm

Distributed Dynamic Routing Algorithm (DDR) [Navid01] is a hybrid approach based on the notion of zone, like ZRP. DDR constructs a forest from a network topology, where each tree of the constructed forest has to be optimal. Each tree forms a zone. After that, the network is partitioned into a set of non over-lapping dynamic zones. Each node periodically computes its zone ID independent of the other. Each zone is connected via the nodes that are not in the same tree but they are in the

direct transmission range of each other. So, the whole network can be seen as a set of connected zones. Thus, each node from a zone can communicate with another node from another zone The size of zone increases and decreases dynamically depending on some network features such as node density, rate of network connection / disconnection, node mobility and transmission power Mobile nodes can either be in a router mode or non-router mode regarding its position in its tree This allows a more efficient energy consumption strategy. Each node is assumed to maintain routing information only to those nodes that are within its zone, and information regarding only its neighboring zones.

The DDR - algorithm consists of six cyclic time-ordered phases preferred neighbor election, forest construction, intra-tree clustering, inter-tree clustering, zone naming and zone partitioning These are executed based on information provided by beacon to its neighboring nodes. The content of beacon is primitive at the beginning, and it gets enriched during each phase of the algorithm. At the beginning, each node in the network topology carries out the preferred neighbor election algorithm. Then, a forest is constructed by connecting each node to its preferred neighbor and vice versa. Next, the intra-tree clustering algorithm is carried out in order to give an appropriate structure to each tree, and build intra-zone routing table for each node. After that, inter-tree clustering algorithm provides a natural structure among trees which is kept in the inter-zone routing table of gateway nodes. Each tree is assigned with a name by executing zone naming algorithm Since the constructed forest contains a set of tree where each tree is assigned with a name, then the network is partitioned to a set of non-overlapping dynamic zones. Note that DDR only uses beacon to construct a forest and to build both intra-zone routing table and inter-zone routing table as well as other phases of the algorithm. Therefore, it avoids global broadcast throughout the network cause a more efficient use of radio resources.

3.18 Mobile Mesh Protocols

The Mobile Mesh Routing Protocol (MMRP) [Grace00] is based upon the link state approach However, it follows the fish-eye approach like in FSR to advertise the link state packets This is unique in the set of the protocols described so far as it attempts to gain access to the wired world, if available Packets over the wired routes are sent encapsulated throughout the wired path MMRP is one protocol in a set of related Mobile Mesh protocols that also includes the Mobile Mesh Link Discovery Protocol (MMLDP) and the Mobile Mesh Border Discovery Protocol (MMBDP). Together, these protocols provide a flexible, extensible mobile adhoc networking capability.

The Mobile Mesh Link Discovery Protocol (MMLDP) provides a media independent mechanism for discovering neighbors in a mobile adhoc network, and is capable of determining whether links are unidirectional or bidirectional. It periodically broadcasts the Hello message which also includes the neighbors interface addresses on which the hello messages were received in last fixed period of time. This way it finds out whether the link is unidirectional or bi-directional It suggests to use some metric but are unspecified.

The Mobile Mesh Border Discovery Protocol (MMBDP) enables a mobile adhoc network to utilize a fixed/wired network for dissemination of routing information and for forwarding of data. Leveraging this collateral flow has a couple of important benefits. First, it can prevent partitions from occurring in the mobile adhoc network, thus improving the likelihood that mobile users can communicate. Second, since wireless networks are typically bandwidth constrained, it allows traffic from the wireless links to be offloaded to the higher capacity wired network. If two or more nodes in a mobile adhoc network each have a connection into a fixed network then by creating a tunnel we can communicate using wired world.

After discovering a peer and setting up a tunnel to it, an implementation of MMBDP starts the Mobile Mesh Link Discovery Protocol on the tunnel interface. MMBDP then adds the tunnel interface to the Mobile Mesh Routing Protocol The tunnel interface appears to MMLDP and MMRP to be just another IP interface, the fact that it is a tunnel interface is not exposed. MMLDP discovers "virtual links" from the tunnel interfaces of other border routers and reports them and their

associated costs to MMRP. MMRP includes in its LSP the IP address of the tunnel interface and its associated links and link costs. Thus, MMRP computes least cost paths that can include both wireless links and "virtual links"

Chapter 4

Effect of Location Information on AODV

This chapter studies how the availability of location information of nodes may be utilized to improve the performance of AODV. One way to make the location information available is to propagate it from a node to other nodes in the network. In future, Global Positioning Systems (GPS) cards may be available in mobile nodes [Imei96]. Therefore, another approach may be to find the location information by querying a GPS-like systems.

Based on the two ways of availability location information described above, two new protocols are designed. The protocol, which is based on packets based location information, is termed Location assisted AODV (LODV). Other protocol, based on GPS like systems, is termed here as GPS assisted AODV (GODV). Both the protocols are applied with the basic AODV protocol. AODV is briefly described in section 3.10. AODV is a work in progress in the MANET working group of IETF. Basic protocol is described in [Perkins99] and the current draft of AODV is available at [Royer01].

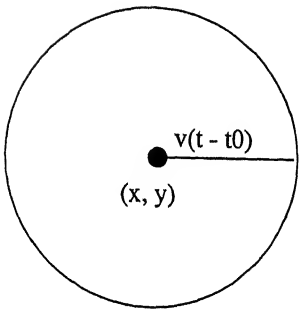


Figure 4 1: Expected zone at some instant t with node moving at velocity v

4.1 LODV

LODV is a location information assisted Ad Hoc On Demand Distance Vector protocol The approach centers around sending Route Request (RREQ) when there is demand (when the node requires) to communicate to some destination in the network The nodes take the guidance of the location information available with the node, when deciding to re-broadcast the RREQs Thus, it restricts the range of the broadcast request region and is expected to reduce the routing overhead. The scheme of using the location information is an idea adapted from Location Aided Routing (LAR) protocol proposed in [Nitin98].

4.1.1 Description of Protocol

A moving node may provide the location information to the other nodes in the network. Thus the expected location of the node can be guessed with the help of the available location information. For example, let v be the speed of the node and let the location information at instant t_0 be available. If the current time is t, then the expected zone in which the node may be found, as shown by figure 4 1, is the area covered by radius $v(t - t_0)$ centered at the location (x, y) at time t_0 Hence, the future route request for this node could be limited to the region covered by the zone This is expected to result in less overhead.

While sending a route request, the source appends the location information in the RREQ packet. It also includes a metric which is the distance of the destination (based on its last known location) from the source at the time the route discovery is

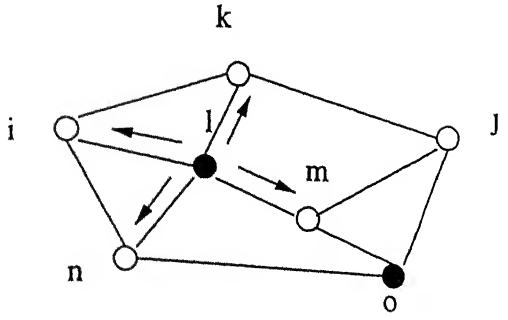


Figure 4.2: Intermediate node closer to the destination

initiated. On receiving a RREQ, an intermediate node checks whether its distance to the destination is less or more than the distance of the destination from the source node. If the distance of the destination at the intermediate node is greater, the packet is discarded, otherwise the packet is rebroadcasted from the intermediate node. The idea is as follows: if RREQ packets reach such intermediate nodes which are closer to the destination on the path, the distance of the source node from the destination via intermediate nodes is expected to be less

It can be seen in the figure 4.2. Let l is the source node and o is the destination node. RREQ packets will be received by all the neighboring nodes i, k, n and m The distance of the node o from the node i is greater than the distance of the node o at the node l. Whereas, the distance of the node o at the node m is shorter than the distance of the node o at the node l. The node i will discard the packet, whereas the node m will rebroadcast the packet. Basically, the idea of the physical "closeness" is employed to restrict the flooding. To make the scheme more adaptive, intermediate nodes may recalculate the distance metric for the source and to itself, whenever more recent location information is available with it. Each RREQ packet contains following location information:

1. The space coordinates of the destination known at the time instant *dst_time.*

2. The space coordinates of the source initiating the route discovery.

3. The speeds of the destination and the source.

4 The distance of the destination from the source at the initiation of the route

discovery. The distance function is calculated on the geographic positions of the source and the destination.

Each Route Reply packets (RREP) packet contains following location information:

1 The space coordinates of the destination

2 The speed of the destination.

3. The time at which the reply is sent.

On receiving a RREP packet, all the intermediate nodes and the source on the route, update the location information for the destination in their respective routing table.

A node broadcasts a RREQ packet when:

- The route to the destination is not known.
- The existing route is broken due to link failure.
- The route expires.

To prevent the storming by RREQ packets, expanding ring search method is employed. The operation of search is controlled with the help of the Time-To-Live (TTL) field. TTL is set to some initial value and an associated timer, route request timer, is set with a timeout value. The value of the timeout is a function of the TTL and the link traversal time. When TTL, which is decremented at each hop, reaches zero, the packet is discarded. In case no reply is received within the timeout, the RREQ is retransmitted with some larger TTL value and a larger timeout. In case no replies occur, the above process is repeated till it reaches a TTL threshold value. After that the TTL is set equal to the network diameter. Even if the reply is not received, the process is repeated for at least RREQ_RETRIES times before the discovery is aborted.

When an intermediate node i receives the RREQ packet, first it checks the TTL value. If TTL has reached zero, it discards the packet. Otherwise, it checks the

timestamp t_{sd} of the location information available at the source and the timestamp t_{id} of the that available with itself Let the RREQ packet contain the distance metric $DIST_{sd}$. Let $DIST_{id}$ be the distance of the destination from node i Then the following algorithm is used to resolve whether and how node i should forward RREQ, or disregard it completely.

1 *If* ($t_{sd} < t_{id}$)

Calculate the new distance of the destination ($DIST_{sd}$) from the source based on the location information available at the node i. Similarly, calculate $DIST_{id}$, the distance of the destination from i based on the location information available with itself.

else

$DIST_{sd}$ is the same as it is in the RREQ packet and $DIST_{id}$ is calculated based on the location information of the destination available in the RREQ packet received at the node i.

2. For a parameter LAMBDA (described later),
if ($DIST_{sd}$ + LAMBDA >= $DIST_{id}$)

Rebroadcast the RREQ packets to the neighbors, replacing the distance metric in the RREQ with the $DIST_{id}$.

else

Discard the packet.

LAMBDA is a function of (*i*) the speed of the destination, (*ii*) the speed of the source, (*iii*) the last known time of the location information of the destination, and (*iv*) the timestamp at which the route discovery was initiated. The value of LAMBDA may be critical, and can affect the performance of the protocol Suppose, an intermediate node is allowed to forward a RREQ only if the distance of the destination from itself is strictly less than that of the destination from the source (LAMBDA is zero) then there may be a situation when RREQ is not delivered

at all. For example, in figure 4 2, if the node m goes down, the RREQ may not reach the final destination Because, the distance of the node o may not be less than the distance at node n or k That is why, LAMBDA is used so that it can give enough robustness to incorporate such situations An appropriate choice of LAMBDA may result in the packets taking the route through node n or node k to reach the destination. The parameter should be tuned appropriately.

This process of rebroadcasting RREQ is repeated at all the intermediate nodes While forwarding the RREQ, a reverse path is created so that the reply can be sent back along it. The reverse path routes are deleted when timeout occurs which is greater than the maximum round trip time (RTT) of the network If any intermediate node contains a fresh enough path to the destination, the RREP is generated by the intermediate node. In this case, the location information is copied from the routing table entry of the node to the RREP packet. Otherwise, finally, the destination replies to the RREQ. It appends its location information in the RREP packet so that it can be used in future route requests.

The protocol assumes that the neighborhood connectivity is ensured all the time To achieve the same it may either rely on the MAC layer or may send periodic Hello messages to the neighbors. In the latter case, non-receipt of a fixed number of Hello message replies, say 2 or 3, from a particular neighbor, is treated as a failure of the link. Similarly, a new Hello message indicates the presence of a new neighbor reachable from the node. A unicast route error (RERR) packet is sent when·

- Any node detects a broken link.
- Any node that does not have route to the destination for which the data packet has arrived to it.
- Any intermediate nodes gets RERR message from its neighbor.

Each intermediate node maintains a list of precursors. The precursors list includes all such neighbors which are using this link on some of their routes. The RERR packet is sent to all the nodes in the precursors list. The unreachable destinations are appended in the RERR packet and the RERR is sent towards the source.

The nodes receiving RERR packets invalidate the route. Using the RERR packets, hence, the protocol limits the possible use of broken links.

4.2 GODV

It is a variant of the LODV scheme It assumes that the location of the destination can be obtained from some source, like GPS systems, by the source at the time of the route discovery The simplest approach in this case is to send the packet in the direction of the destination. To achieve it, each node may also maintain the direction of the link along with the neighborhood connectivity in the routing table. When a node requires to send the packets to some destination, it can choose the link in the direction of the destination. Hence, it can limit the route requests in the direction of the destination. However, this approach may not often work in practice. Two such cases are illustrated by figure 4.3.

- The node does not have connectivity in the direction of the destination In the example figure, node 2 and 3 have connectivity with the source node 1. Let the nodes forward the packet if the destination node falls in the interior of an imaginary ray centered at some neighboring node that forms an angle of $\pi/6$ from the segment representing the neighbor link In this situation, the packets for the nodes 7 and 8 will not be delivered

- If the node 1 forwards the requests along the direction of the shortest path only (through node 2), node 2 will not be able to forward to any of the destination nodes node 5 or node 6. We may conclude that there is no path available or the node is down, whereas the paths may be available. For example, there are paths $1-3-4-6$, $1-3-4-5(-6)$ or $1-2-3-4-6$.

The scheme presented here, does not assumes any such attachment of the direction with the link. Instead, it uses the property of the physical "closeness" as described in the previous section. It calculates the distance of the destination from the source and takes the decision of rebroadcasting the route request packets in the manner similar to the one described in the previous section

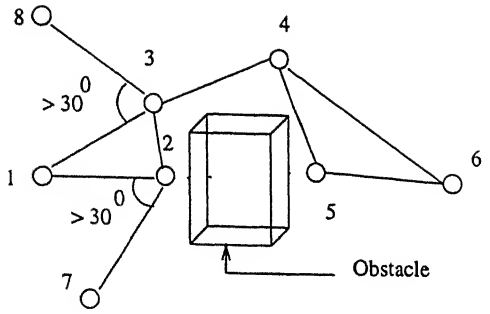


Figure 4.3: Destination node obstructed by a building

The sender initiates the Route Request and sends the following location along with the packet:

1. The geographic coordinates of the destination.
2. The timestamp of the destination
3 The geographic coordinates of the source.
4. The speeds of the destination and the source.
5. The distance metric for the destination from the source

Route reply packets do not contain any extra information The location of the destination node is queried only once by the source. Each query takes a finite amount of the time. The rest of the nodes use the information in the packet received from the source. The receiving intermediates nodes decide to rebroadcast the RREQ as it is described in the previous section. The intermediate nodes with better location information are not incorporated to contribute to avoid the latency associated with each location query.

If the $DIST_{id}$ is less than the $DIST_{sd}$ within the offset parameter LAMBDA, the packet is rebroadcasted. Otherwise, the packet is dropped The value of the LAMBDA is again the function of the speed of the destination, speed of the source, location of the source and the location of the destination. The rest of the scheme is very much similar to the one described in the previous section

4.3 Simulation Model

This section describes the simulation model used to evaluate the performances of the protocols . The simulation is run on the *ns-2* [Fall00] simulator For the purpose of the simulation, AODV protocol implemented in *ns-2* has been modified to incorporate the changes which have been proposed in the recent draft (version 07) of the protocol. However, a few features, for example route reply acknowledgement, interface assumption, and Hello messages are not used The physical layer and the link layer components in *ns-2* are the same as provided by the CMU monarch extensions [Monarch98]. A brief description of the model is presented below.

1. The Radio Propagation Model is assumed to be the Two Way Ground Reflection Approximation in which (*i*) Friss free-space attenuation ($1/r^2$) at near distances, and (*ii*) an approximation to Two Way Ground ($1/r^4$) at far distances is assumed. The approximation assumes mirror reflection off a flat ground plane.

2. The antennas are assumed to be a unity gain omni directional antenna That is the antenna loses equally in all directions at unity distance

3. The Network Interface implements a shared media where each node can over hear packets transmitted by other nodes of the network subject to the collisions and the propagation model. The parameters reflect the Lucent WaveLan Direct Sequence Spread Spectrum (DSSS) radio interface. This radio model has bit-rate of 2 Mb/sec and a range of 250 meters.

4. The Medium Access Control protocols, the IEEE 802.11 Distributed Coordination Function (DCF) MAC protocol is provided. It uses Request-To-Send (RTS) and Clear-To-Send (CTS) control packets for unicasting data transmission to the neighbors. Hence it uses "RTS/CTS/Data/ACK" pattern in "unicast" packets. This mechanism ensures that the channel is reserved before data transmission and avoids hidden station problem by implementing virtual carrier sensing. For "broadcast" packets physical carrier sensing is used. CSMA/CA scheme is used to transmit the broadcast packets.

A detailed description of the simulation model can be found in [Broch98] and [Monarch98]

The routing agents receive all the data packets transmitted or forwarded and the protocol takes appropriate action on receiving the packets The protocols assume feedback from the MAC layer to report the link breakage For example, not receiving CTS after RTS or no ACK after Data packets may be considered as a link break Other network layer tactics such as *Hello* Messages are not used RREQ packets are considered as broadcast packets, whereas RREP and RERR packets are treated as unicast packets. For data packets, a *buffer* of capacity 64 is used. *Buffer wait time* is 50 seconds. All the packets are queued at *interface queue* while waiting for the MAC to transfer the packets. The *interface queue* is of capacity 64. The control packets take priority over the data packets and queue model is assumed to be FIFO

4.3.1 Connection Pattern and Mobility Models

The connection pattern is generated with the tool *cbrgen* available with the *ns-2 tarball.* All the data packets are CBR (continuous bit rate) packets. The tool generates random source-destination pairs spread over the network Data payload is of 512 bytes. The number of source-destination pairs is varied to change the load on the network.

Similarly, mobility model is generated by the tool *setdest* available in the *ns-2 tarball.* It generates the random positions of the nodes in the network and further mobility in the network. The rectangular field configuration is 1500x300 with 50 nodes. Each node moves with randomly chosen maximum speed up to 20 m/s. After reaching the destination the node begins to move again after *pause time.* Hence the pause time implies the level of the mobility in the network. Simulations are carried out for highly mobile network to the low mobile network. The simulation runs for 900 simulation time units at each run. Each data point represents an average of three runs. The same connection pattern and mobility model is used in simulations to maintain the uniformity across the protocols

One set of experiments consists of 10, 20, 30, and 40 sources in 50 node network model. In each set, the sources generate CBR data packets (of size 512 byte) at 3

packets/sec packet rate.

In all the simulation studies, we came across in literature high packet rate traffic has been assumed In a non-trivial computation this may be a natural traffic pattern, but for the applications on MANETs (section 1 5) low packet rate traffic may not be an exception. Though there has been significant increase in the bandwidths of the wireless networks, it is still much less than that available in the fixed networks So the applications designed for it may be context-aware, and relocate computation to avoid sending messages very frequently. Thus, it is not unreasonable to assume that many applications exhibit the low packet rate traffic. So another set of experiments has been carried out to model low packet rate traffic network, where a packet is generated every 4 second by the sources

4.3.2 Performance Evaluation Criteria

The performance evaluation is based on the comparison of following metrics·

- *Packet Delivery Fraction (PDF)* : The ratio of the data packets delivered to the destination and the total number of data packets generated by the sources.
- *Average Delay (AD)*: It is an aggregated average of the time taken by a packet for the successful delivery at the destination. The time for the successful delivery is the interval between between the packet is generated at the source and the time when it is delivered to the application at the destination. Hence, it includes all the delays that can occur due to waiting in data buffer, in network interface queue and the time taken in propagation.
- *Routing Load(RL)*: It is the ratio of the routing packets generated to the data packets delivered at the destination.

These parameters reflect the efficiency of the protocol and are discussed in detail in section 2.4 and in [Perkins00].

4.4 Performance Evaluation

For the sake of the convenience in evaluating performance, the mobility range is divided into three parts

- The region between the pause time 0 to 150 termed further as high mobility region.
- The region between the pause time 150 to 450 termed further as moderate mobility region
- The region beyond 450 termed as low mobility region

Figure 4.4 and 4.5 show the packet delivery fraction for high packet rate traffic and low packet rate traffic.

- In high packet rate traffic, LODV performs similar to the AODV for less number of sources but the performance is better, between 10 to 30 percent, for higher number of sources, particularly in moderate mobility region.
- In low packet rate traffic, its performance is significantly better than AODV (about 10 to 40 percent) for all the sources.
- The performance of GODV is worse for less number of sources for both the types of traffic, otherwise it performs significantly better (about 10 to 80 percent) as the number of sources increase.
- For low traffic, overall performance of LODV is better than GODV (about 5 to 20 percent).

GODV has more accurate information regarding the location of the node That is why it performs better for both the types of traffics when there are many sources. In case of LODV, the location information is available after an initial connection establishment. It can help in subsequent route discoveries only. Also, the location information may become incorrect with mobility of network and the speed of the destination. Hence, at lower mobilities it results in slight increase in PDF at high

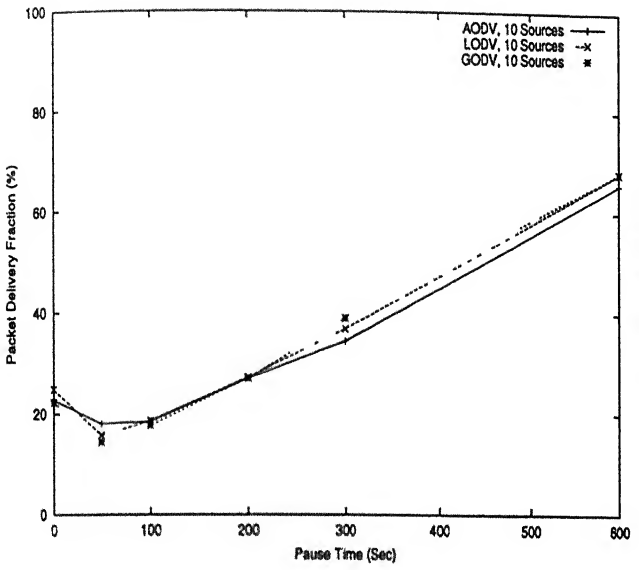
packet rate. At high packet rate, if the path is not discovered in time, the packets are dropped at send buffers and interface queues So the stale location information does not help much. Whereas, the GODV has better information, and, hence is able to take the advantage of it. At low packet rate, the packets are generated slowly and hence LODV is able to absorb more time spent on discovery cycle Due to this, LODV performs significantly better in low packet rate traffic As the number of sources grow, chances of getting correct location location information due to the adaptive nature of the protocol increases and hence LODV performs better

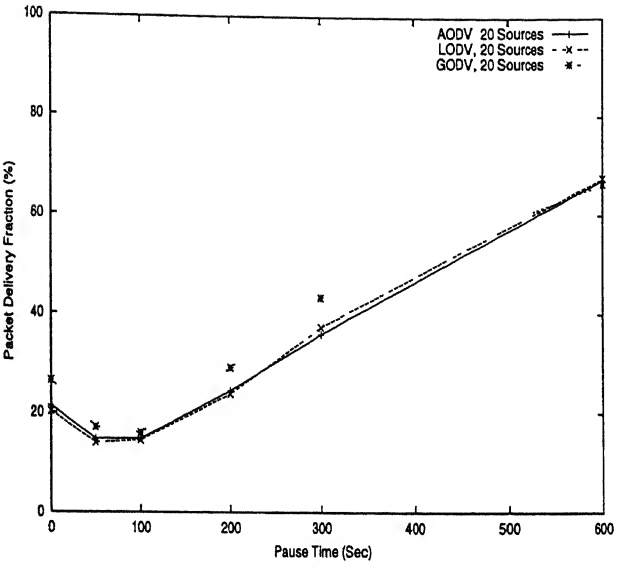
Figure 4.6 and 4.7 show the routing load

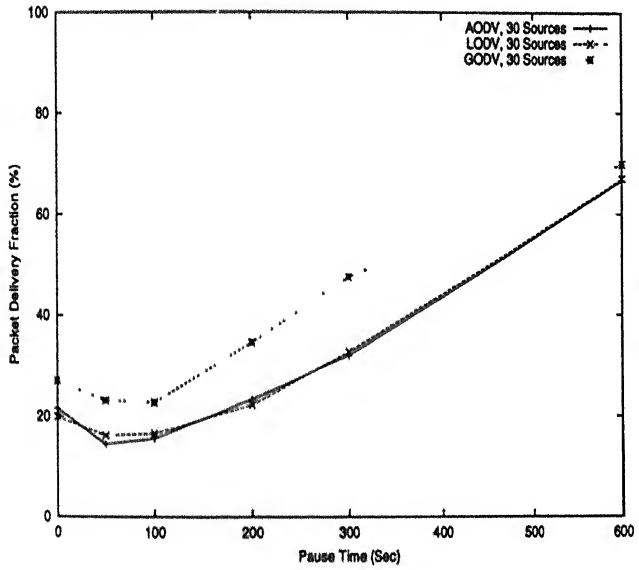
- For high packet rate traffic, for 10, 20 and 30 sources, RL of the LODV roughly the same as of the AODV. But for 40 sources, its RL is better of the factor 1 to 1.5, in high mobility region and low mobility region
- In low packet rate traffic, the RL of AODV is higher except for 40 sources.
- For high packet rate traffic, GODV has more RL than both the protocols (factor ranging from 1 to 3). However, in low packet rate traffic, its RL is remarkably less than AODV (and LODV).
- At high mobility, the expanding ring search combined with the location guided search, result in increased routing load. With each timeout, the TTL value is increased which eventually results in increased load and average delay.

Figure 4.8 and 4.9 show the Average Delay.

- GODV has significantly higher average delay (usually of factor 1-5) than both the protocols. The difference is larger in the high mobility region.
- The average delay of LODV turns out to be better as the number of sources increase (by a factor of 1 to 2).
- In low traffic, the delays for both the protocols are higher than the delays for AODV for all the sources. The difference widens with the increase in number of sources.







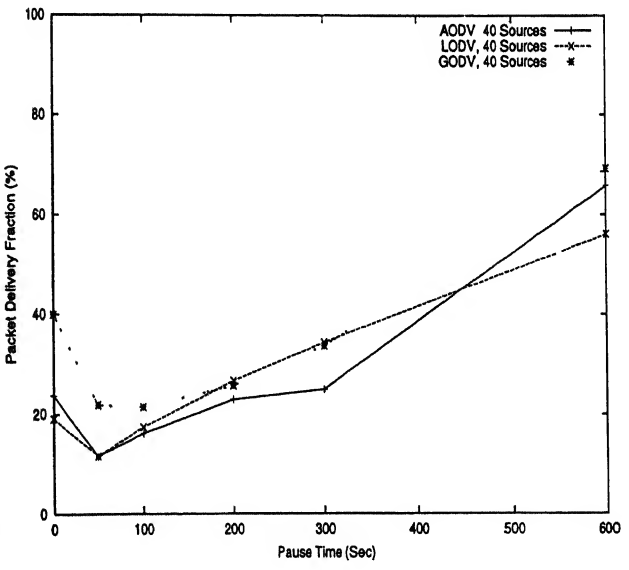


Figure 4.4: Packet Delivery Fraction at High Packet Rate

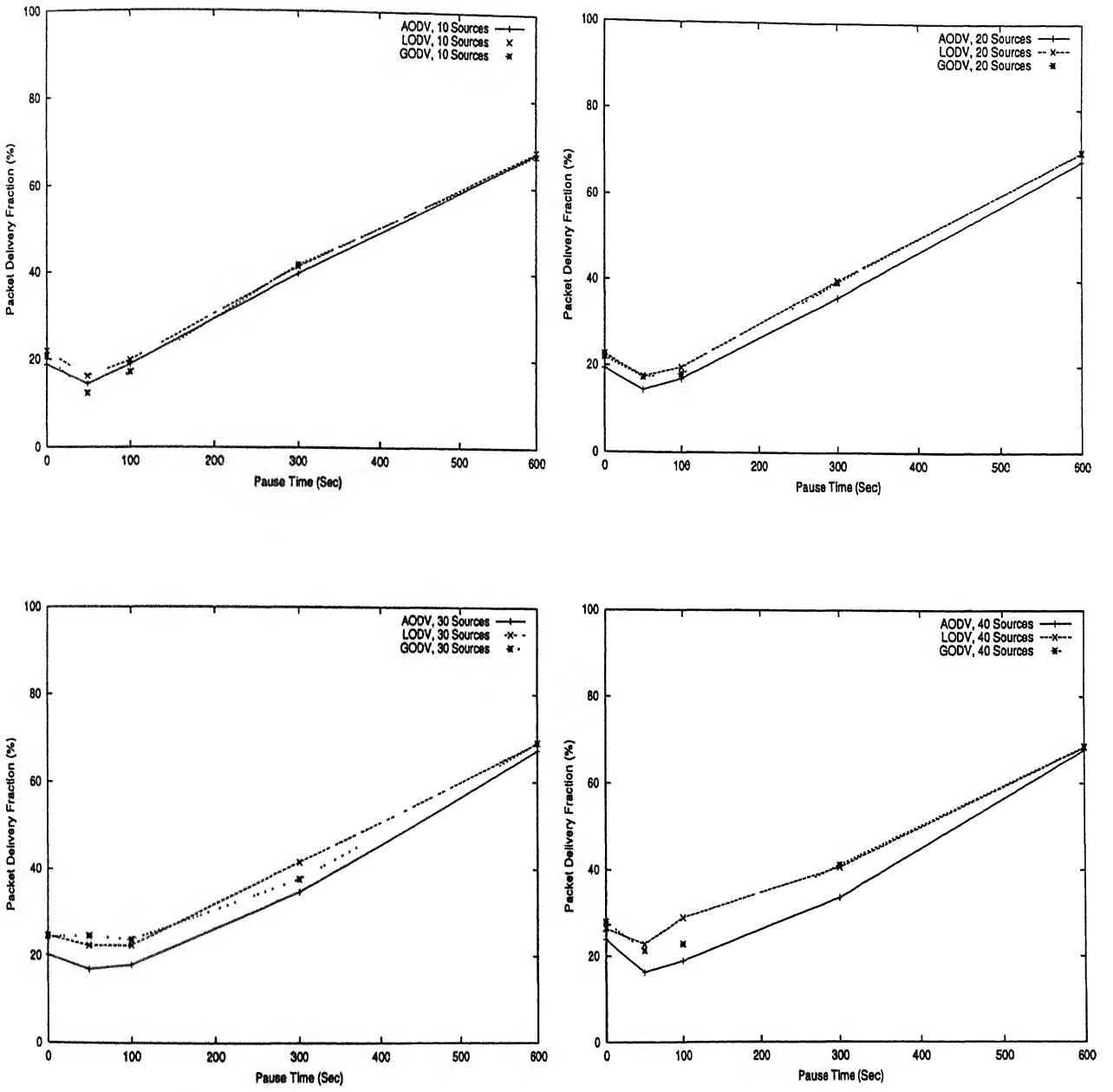


Figure 4.5: Packet Delivery Fraction at Low Packet Rate

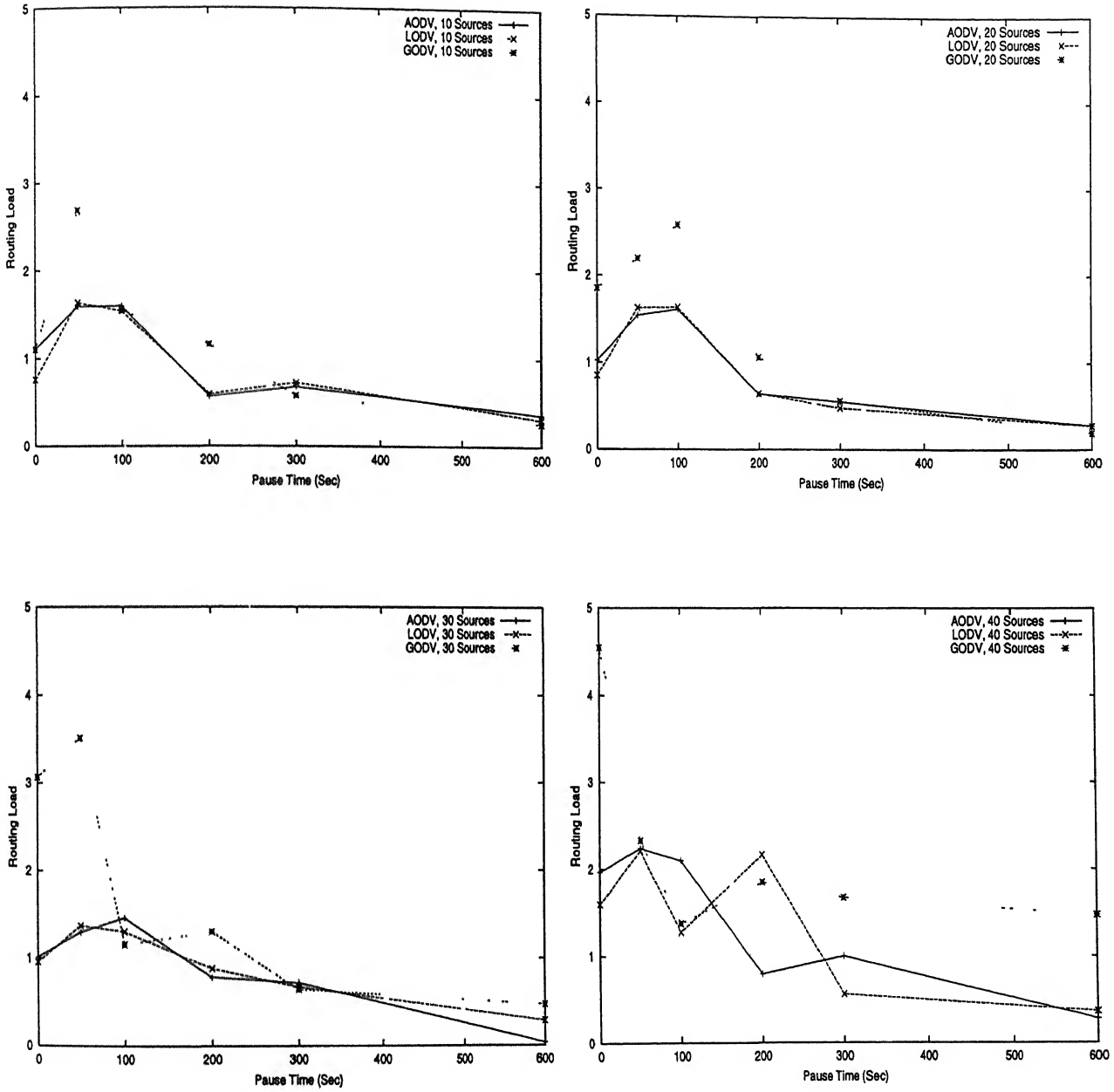


Figure 4.6: Routing Load at High Packet Rate

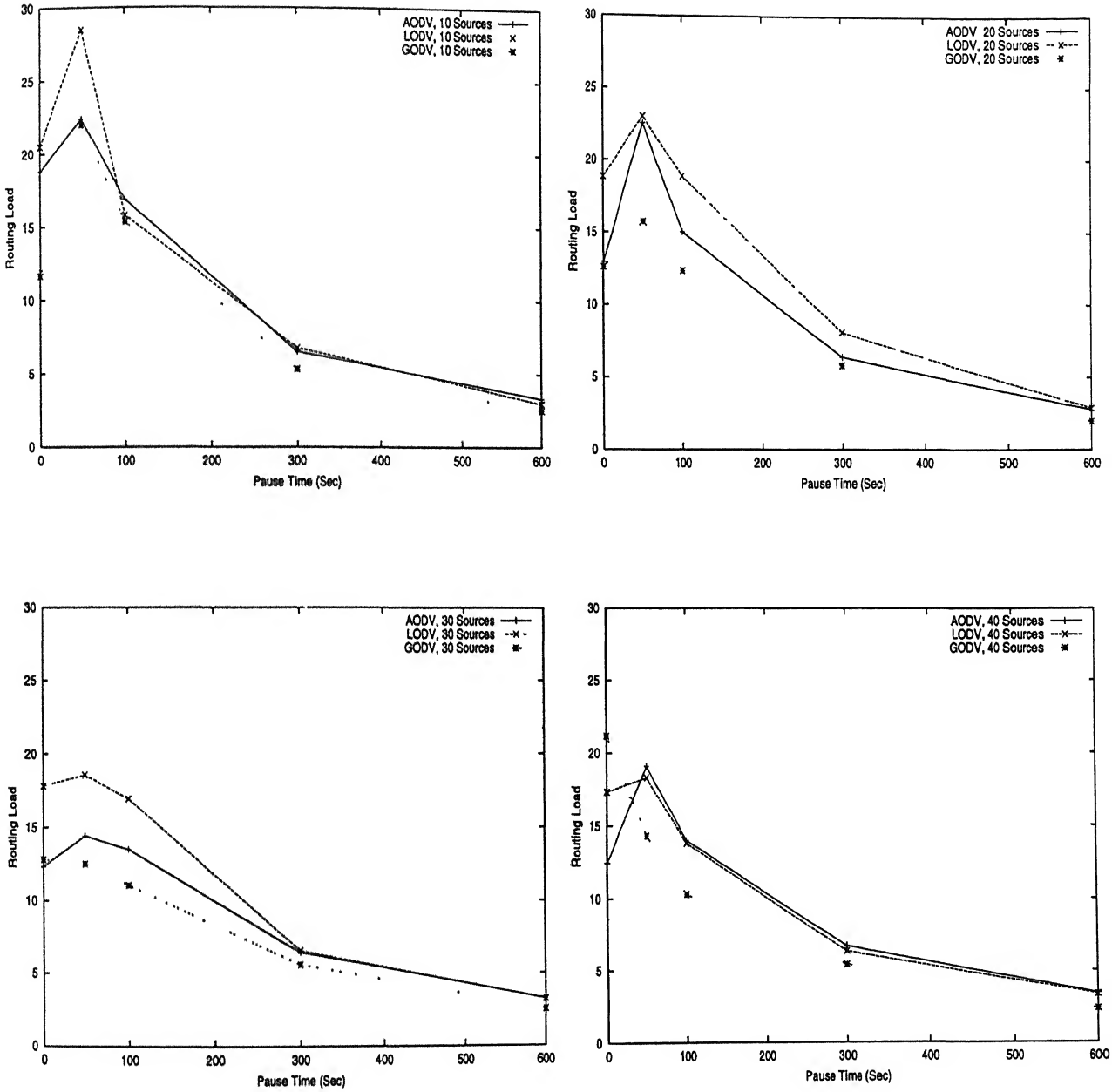


Figure 4.7: Routing Load at Low Packet Rate

- In low packet rate traffic, LODV has better delays than GODV except in very high mobility where GODV performs better

GODV takes 20 ms second in getting the location information which is an extra overhead, for each route request. It increases overall end-to-end-delay LODV has better delay at average mobility particularly for moderate mobilities in high packet rate traffic It is able to discover the paths more quickly and hence there is less delay However, in low packet rate traffic, the increased packet delivery results in increased delay. As the chance for the packets waiting in the queues become more

4.5 Summary

The results show that using location information, if available, can be advantageous In cases where it gives similar packet delivery it results in lower latencies. For low and moderate mobilities, it often results in better packet deliveries and routing load. However, at certain high mobilities, the performance is worse than AODV protocol.

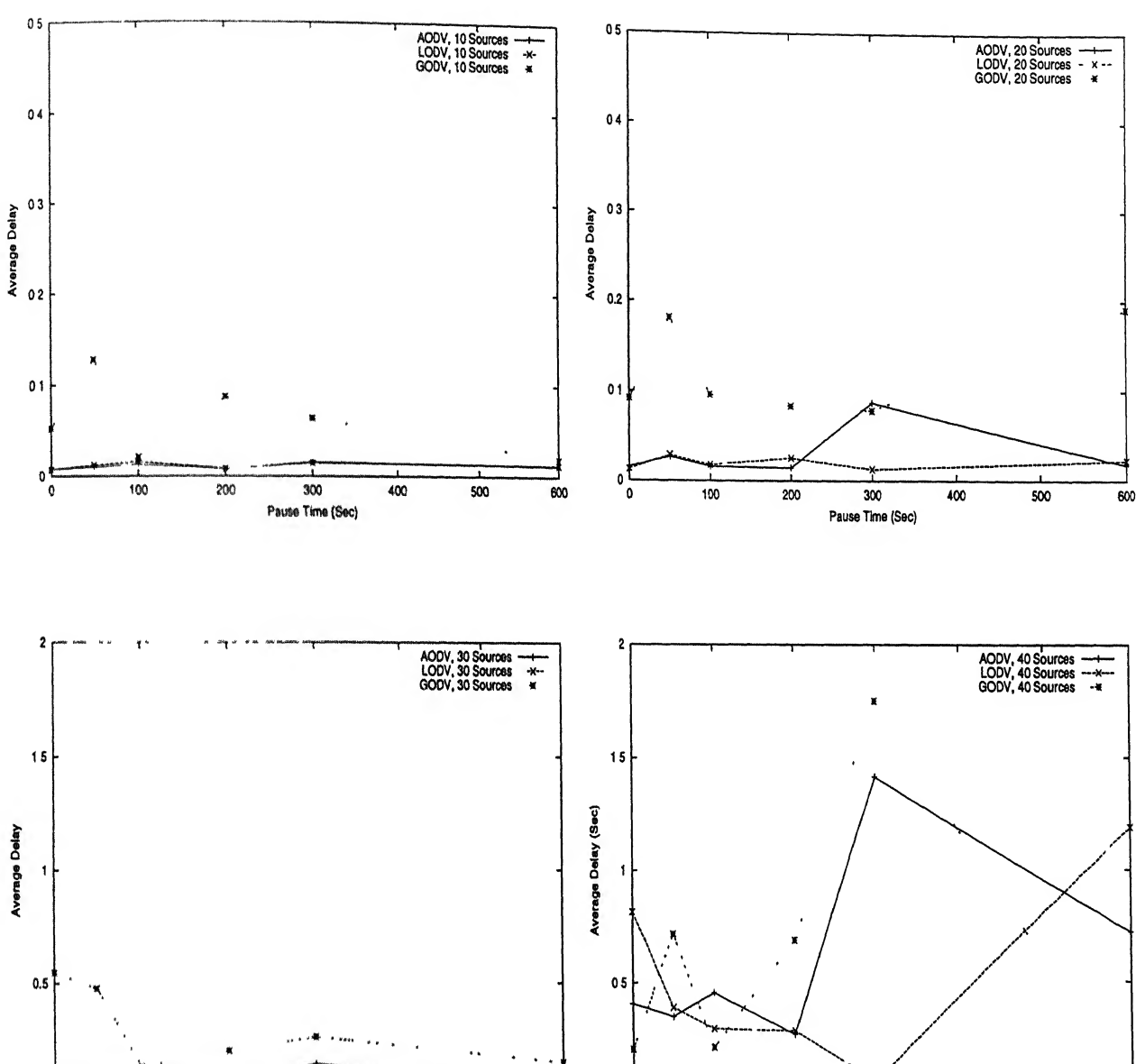


Figure 4.8: Average Delay at High Packet Rate

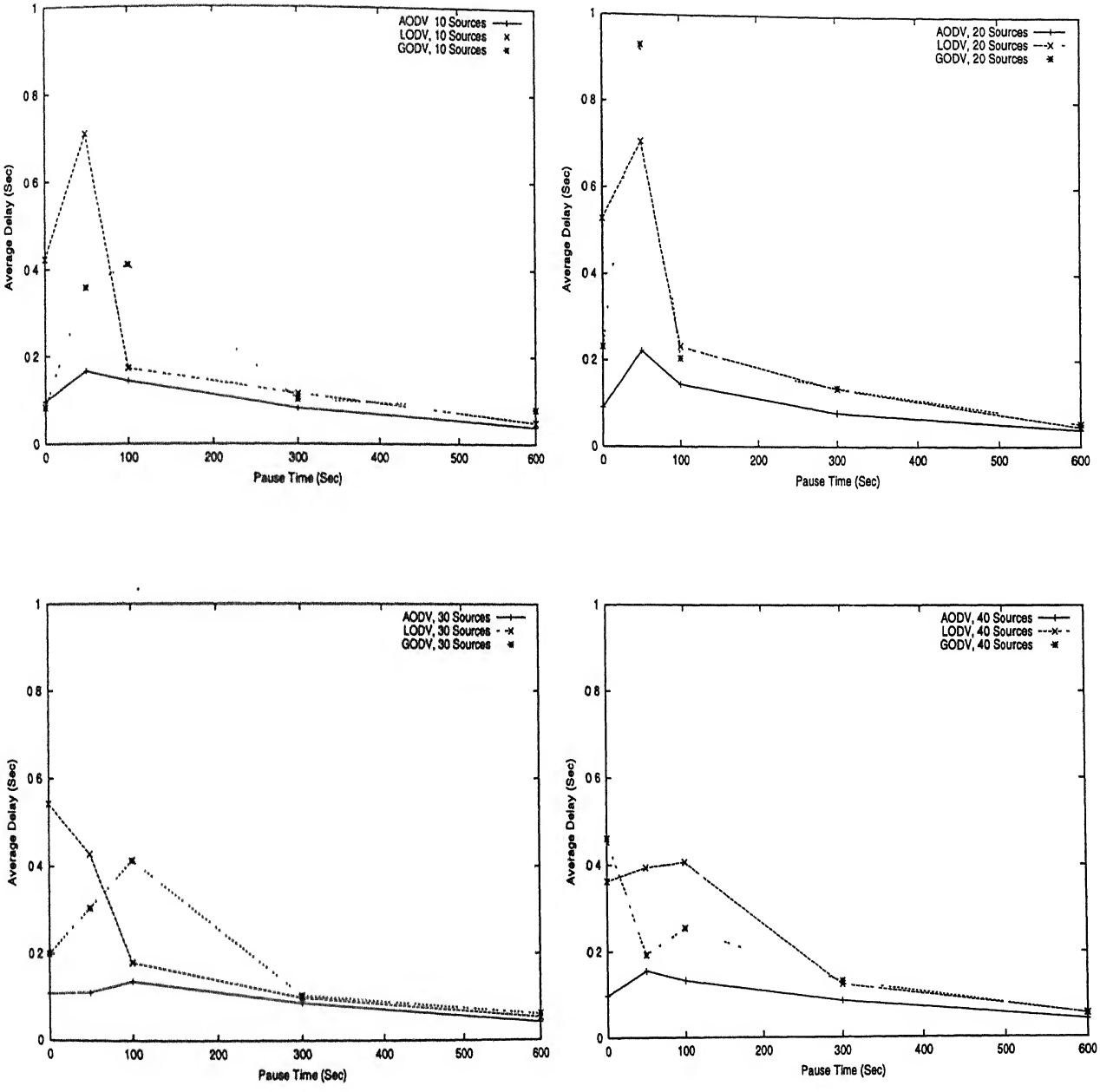


Figure 4.9: Average Delay at Low Packet Rate

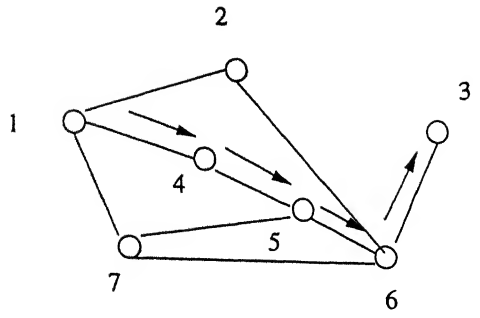


Figure 5.1: RREQ Packets Flow for a Destination

conservative approach which restricts some of possible optimizations, which may improve the performance of the protocol. One such situation where the optimization may be achieved is described below.

In the figure 5.1, a path from node 1 to 3 is shown which is active Consider following two cases:

1. The intermediate nodes, for example node 4, node 5 or node 6 want to communicate with the node 3. In this case, all the nodes will be able to get a down stream route as there is a active route to the destination. Since the route entries are destination oriented, these nodes are able to take the advantage

2. The source node 1 wants to communicate to any intermediate node (node 4, node 5 or node 6) on the path. In this case, the path is not available because the entry in the respective routing tables are associated with the address of node 3. Hence, the route to these destinations will not be found in the routing tables and the route discovery cycle has to be initiated to get the path. During discovery, intermediate nodes will not reply because the sequence number in their entries will be less than the sequence number in the packet.

If such cases can be utilized, it may improve the performance of the protocol. The protocol, referred as AODV-C, incorporates this idea. The basic idea is to send the source route along with the route reply as done in DSR [John96] The intermediate nodes and the source node cache the source route path in the routing table corresponding to the route entry. Before flooding the request packets, each

node checks whether the destination of the RREQ is on any of the route currently going through the node. If so, the packets are routed without route discovery cycle.

5.1.1 Protocol Description

For route discovery, route request and route reply packets are used The RREQ packets is very much similar to the RREQ packets of the AODV RREQ packet are flooded in the network and the intermediate nodes forward the requests. The operation is controlled by the expanding ring search method When the destination gets the route request, it unicasts the route reply packets back to the source. The route reply packets accumulate the nodes on the route The nodes, receiving the route replies copy the source route in the routing table corresponding to the entry for the destination. Before forwarding the reply, it appends its address in the route reply packet.

On subsequent requests, the node checks its for the availability of the the intended destination of any route cached in its routing table. If the entry is found, the packet is forwarded to the next hop. Otherwise, the route discovery is initiated.

The extra packet overhead is proportional to the number of the nodes on the route. The addresses of the node are not long, for example in case of IP addresses are 4 bytes long. The number of the nodes on the route is limited with the network diameter. For example, in case of 30 hop network, 4 byte addresses will result maximum of $30 * 4 = 120$ bytes of overhead with the route reply. Average paths will be far less than the network diameter. Hence, the overhead due to source route is not high. The memory requirements are more in case of the nodes near the source. Again the extra memory requirements will be limited with the number of the nodes on the route. However, it will require more computational time. The search time is dependent upon the number of connections currently going through the node and the number of nodes in each path down the stream upto the destinations. In case of failed search, it will have to go through the complete routing tables. However, as the number of the active route going through a node may not be large and hence, it will not incur large overhead.

5.1.2 Simulation Model and Performance Criteria

The simulation model used to simulate the results are the same as it is described in section 4.3. Similarly, the connection pattern and the mobility models are the same as described in section 4.3.1 All the simulation are taken for the 10, 20 and 30 sources for both types of traffic conditions The criteria of evaluation of the protocol are again the packet delivery fraction (PDF), the routing load (RL) and the average delay (AD)

5.1.3 Performance Results

Figure 5.2 and figure 5.3 show the Packet Delivery Fraction for high and low packet rate traffic respectively. In both the cases, there is significant increase in the packet delivery fraction.

- The increase is upto 50 percent in case of large number of sources at high packet rate.
- At low packet rate traffic, the increase ranges upto 35 percent.

The optimization feature on which it works, is more prelevant as the number of the sources grow. Thus, AODV-C performs significantly better than the AODV protocol.

Figure 5.4 and 5.5 show the average delay per packet for high packet and low packet traffic.

- Average delay is higher for both the types of traffics at all the sources. In high packet rate traffic, with the increase in the number of sources, the difference in latencies widens. The increase in delay is usually of factor 1-5 over AODV
- In low packet rate traffic, the average delay is high (a factor of 1-3).

However, with increase in number of sources the delay difference is very much similar for low and moderate mobilities. The difference in delays are more pronounced at very high mobility. However, the increase in delay is expected. As the packet delivery fraction increases, the delay increases due to possibility of increased time in waiting

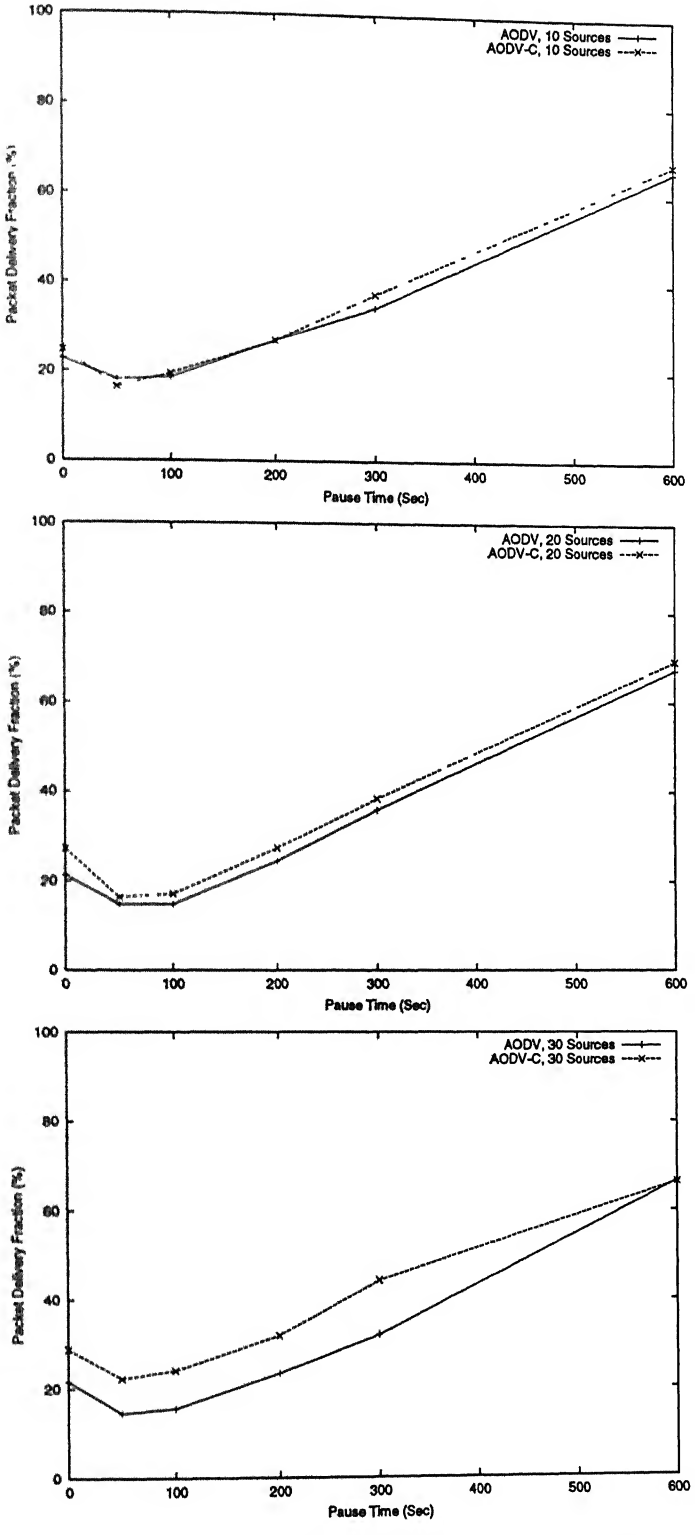


Figure 5.2: Packet Delivery Fraction at High Packet Rate

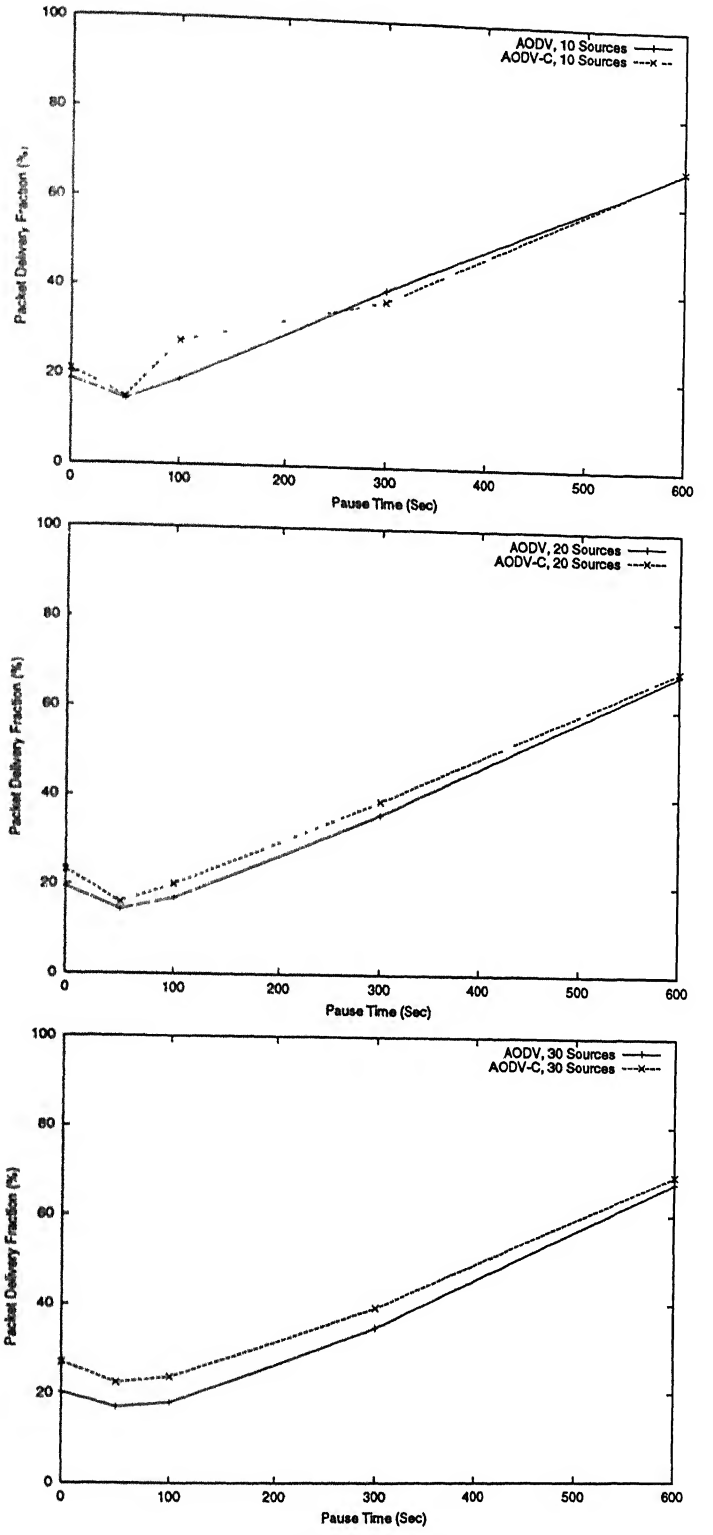


Figure 5.3: Packet Delivery Fraction at Low Packet Rate

in send queues, interface queues or even in propagation at higher number of sources. That is why, expectedly, the latency grows as the number of sources increases In low packet rate traffic, the latency due to route discovery cycle is more pronounced than the other reasons of delay. The increased size of the route reply packets take large transfer times. As the sources grow, the savings of route discovery offset the increased delay due to high packet delivery. Thus, at low and moderate mobilities the latencies are comparable. But at high mobilities, overall delay is increased

The routing load is shown in figure 5.6 and 5 7. As the number of sources increase the RL increases significantly usually by a factor of 1-5 over AODV in high packet rate traffic. In a low packet rate traffic, the RL is comparable at moderate and at low mobilities. However, for very high mobilities, the RL is higher by a factor of 1-2. The chances of the route being correct is much less than the route being broken. With increased PDF and broken links, more control packets are generated. It increases with the increase in the number of paths.

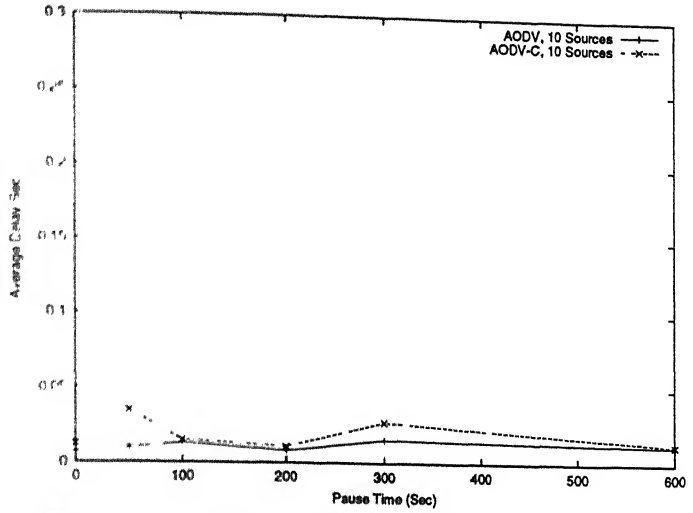
5.1.4 Summary

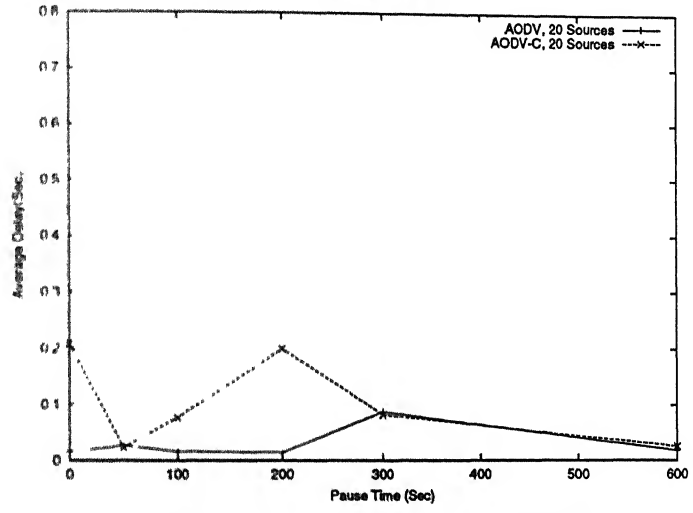
AODV-C results in significant increase in packet delivery fraction. The latency values increase expectedly. But routing load, at high mobility is significantly increased. At moderate mobility, however, the it is similar. The protocol can be used in the cases where PDF is of primary concern than bandwidth.

5.2 Local Repairs in AODV

In MANETs, the link breakages occur frequently due to the mobility. The reactive protocols maintain the routing information on demand and for active routes only. When the links break, the route discovery cycle has to be reinitiated by such protocols to maintain the active routes. The following observations are worth mentioning for reactive protocols:

- Each route discovery takes a finite amount of time. Thus, each route discovery increases the overall end-to-end delay.





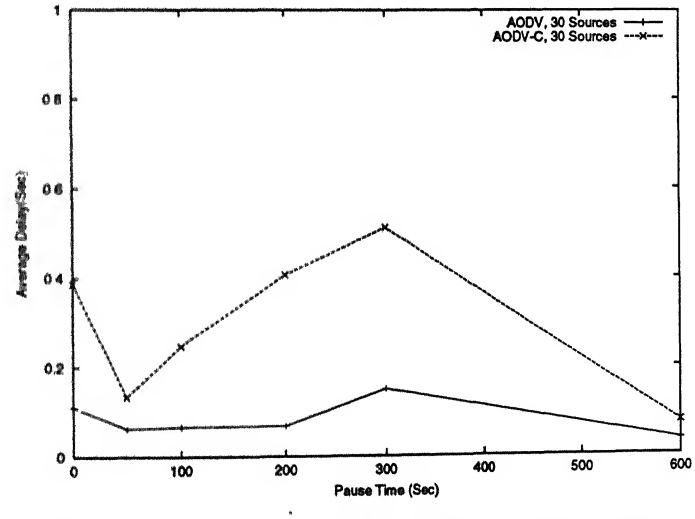


Figure 5.4: Average Delay at High Packet Rate

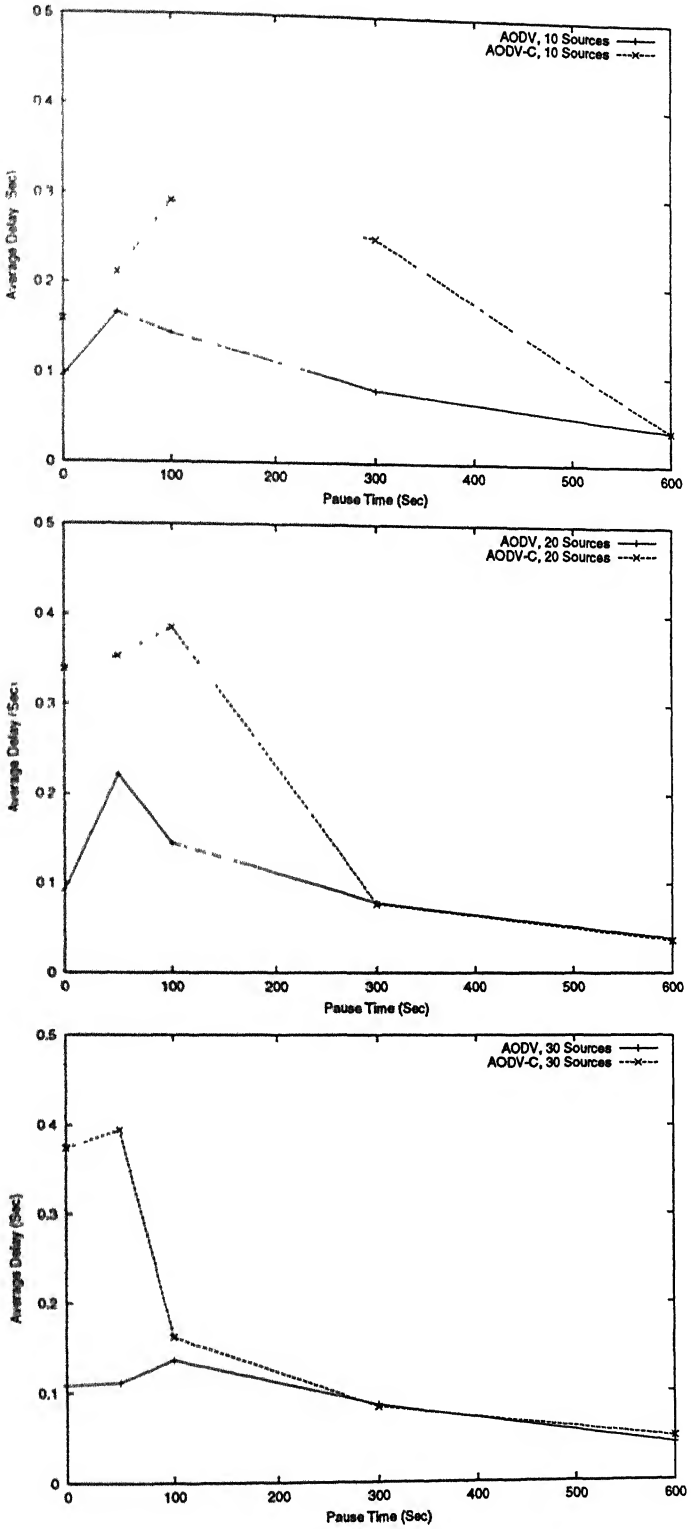


Figure 5.5: Average Delay at Low Packet Rate

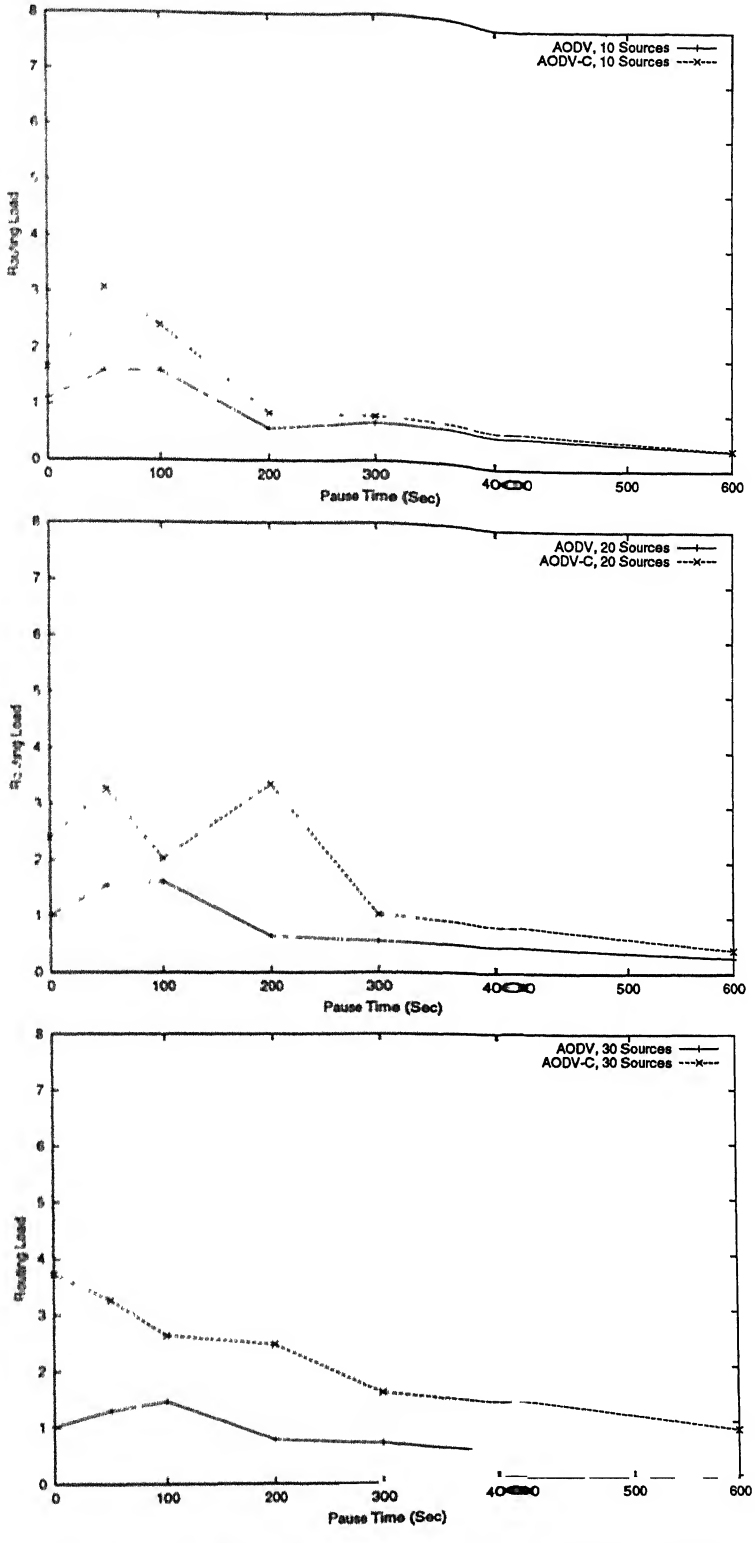


Figure 5.6: Routing Load at High Packet Rate

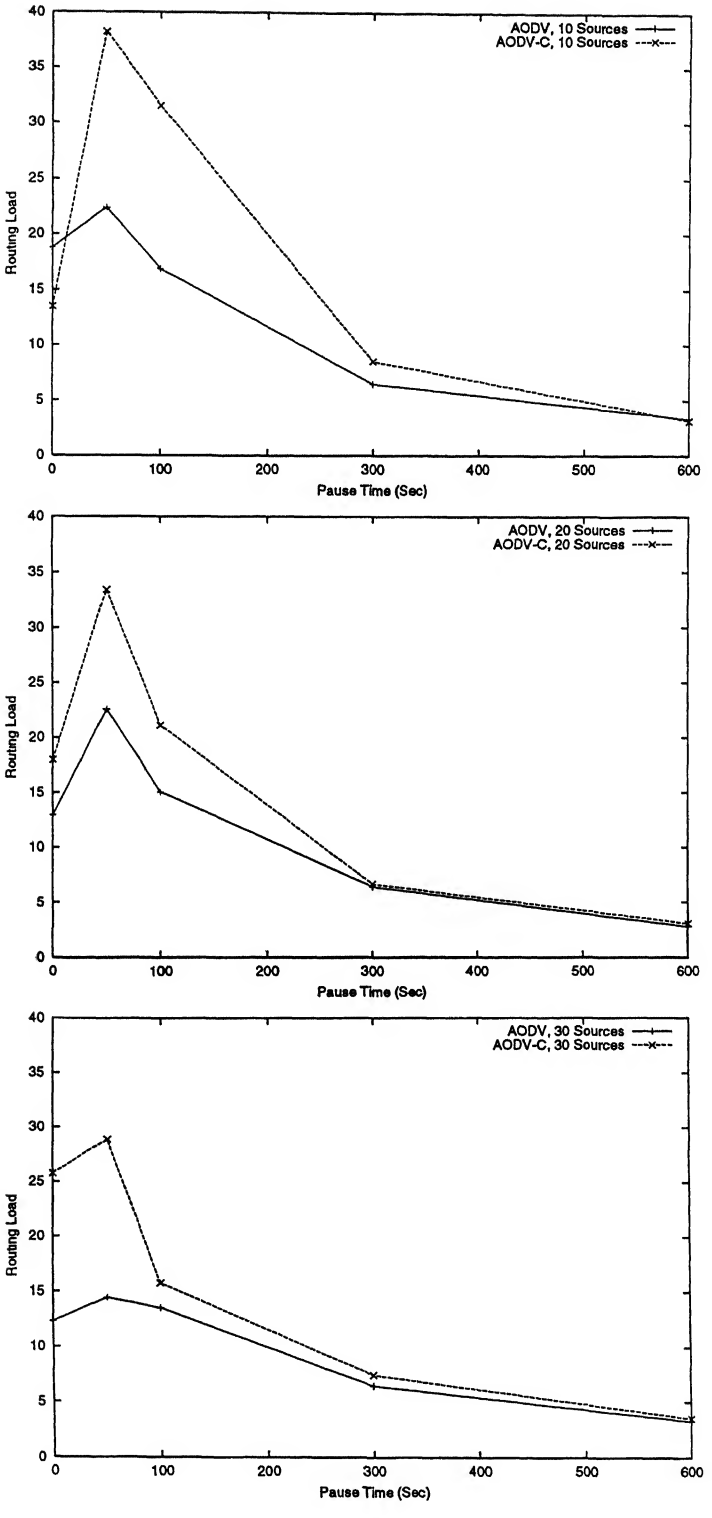


Figure 5.7: Routing Load at Low Packet Rate

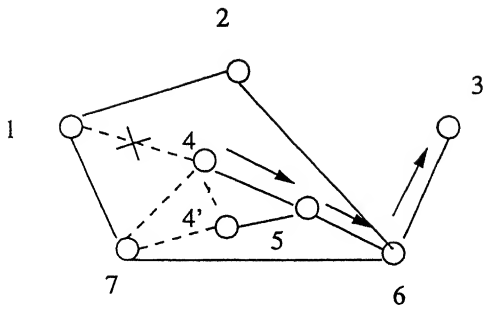


Figure 5 8 Link Failure in a Path

- Since the nodes of MANETs, often have less memory, the queues do not have large capacities. The packets, waiting for the routes, are dropped if the queue becomes full.

- In a complete path, often, very few links are broken. If such links can be repaired, that is, if a compensatory intermediate path could be found quickly, it will result in less latency than that could be incurred in the complete route discovery

A local repair scheme can be used to patch-up the broken path. In AODV protocol, the local repair scheme is follows

Initiate the local repair process, if the node at which the link is broken, is closer to the destination For example, if the hop distance to the destination from the node, at which the link break has occurred, is less than the one third of the total hop length of the path, the local repair is initiated The chances of link failure at any time is equally likely in all the parts of the the link. Since the scheme repairs the path only when the link breaks in one third part towards the of the path. The local repair is not employed to repair the links in first two third part of the path. It restricts the possible optimizations which could have occurred and hence the performance of the protocol.

There is another important observation with regard to the link breakage. Consider the case, when very few links of the route are broken, large part of the route remains the same These paths are not utilized in further route request because the intermediate nodes will not reply to the RREQ packets due to the strict ordering of

the destination sequence numbers. For example, in figure 5.8, if the link $1-4$ goes down, future RREQ packets will not be replied by the intermediate nodes 4 or 5. Lets consider two cases when the link becomes unavailable

- The link from 1 to 4 fails,
- The node moves to a new position and the topology changes For example, the node 4 moves to portion 4'. Due to this the link 1-4 fails and a new link between node 7 to node 4 appears.

In both the situations, AODV will reinitiate the route discovery. If the patch path from 1 to 4 can be found, for example 1-7-4, significant work can be saved. A scheme is presented here to exploit such potential optimizations. This protocol, referred as AODV-L, tries to patch up the path in the scenarios described above.

5.2.1 Description of Protocol

It treats the RREQ packets for the local repair differently from normal RREQs used for route discovery. A flag is set to indicate the local repair packets in the header of the RREQs. The local repair RREQ uses the sequence number one more than the last known destination sequence number of the path in RREQ packets. On receiving the RREQ packets, each intermediate node checks whether it has a path to the destination. If so and the sequence number of the path at the node is just one less than the sequence number in the RREQ packet, it sends back a RREP to the source of the local repair packet. At the same time, it sends a RREP to the original destination. The local repair timer is started at the initiation of the local repair. The timeout value is the function of the number of the hops on the route. The timeout value is tunable and its choice will affect the performance of the protocol. If the path is not repaired within the timeout, the node will send a RERR packet towards the source. On receiving the RERR packet, the nodes invalidate the route.

The scheme is able to solve the possibility of the conflicts which may occur due to the inconsistent destination sequence numbers on the route The part of the path near the destination will have the recent most sequence number if a local repair is

successful. If the local repair has not been successful, the route will be invalidated by the RERR packet sent after the timeout interval. So the sequence numbers on the path at each intermediate nodes form a monotonically increasing sequence While repairing, the sequence may not remain monotonic but settles down within the local repair timeout value and half of the RTT of the path Hence, for an active route, the ordering is always preserved. Otherwise, the route expires and the new route discovery will is initiated irrespective of the previous sequence numbers

Another observation worth mentioning is that in case of multiple link breaks, the local repair scheme becomes recursive. Though, it either ends up with a successful repaired path or timeouts at the first node on the route, which initiated the local repair, instills a new route discovery cycle by sending RERR back to the source.

5.2.2 Simulation Model

The simulation model used is similar to the one described in the section 4.3. Due to the large memory requirements, the packet rate for the high packet rate traffic is assumed to be one packet per second. The mobility model is identical as described in the section 4.3.1. Similarly, the metrics to evaluate the performances are the same, that is, the packet delivery fraction (PDF), the routing load (RL) and the average delay (AD).

5.2.3 Performance Evaluation

Figure 5.9 and figure 5.10 show the PDF. The performance of AODV-L is very much better than AODV for both the types of traffic. The large difference lies in the fact that, whenever a link fails, the path is locally repaired immediately. Further, the local repair time is often significantly less than the latency of the complete path discovery. This, saving in time, results in less packet being dropped at queues. An important observation is that as the number of sources increase, the PDF increases slightly in case of AODV-L, while in case of AODV, the PDF decreases. The route which is not expired can help in finding routes. The active routes are repaired and hence the later requests may find the route without the route discoveries. As the

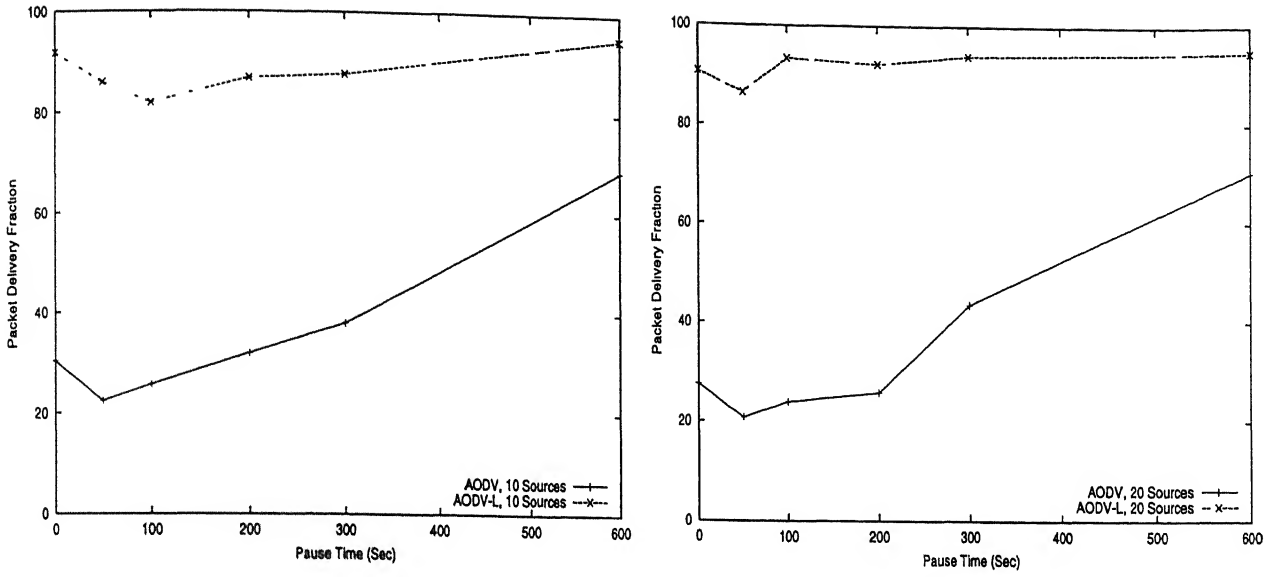


Figure 5.9: Packet Delivery Fraction in a 1 Packet/Sec Network

number of sources increase such cases will increase and hence the better PDF. In case of AODV, the route, which can be found, will often be broken and hence it will initiate route discoveries after traversing a part of the path. It will increase the wait time and hence more packets will be dropped.

The average delay graph is shown in the figure 5.11 and 5.12 for both the types of traffic. For 10 sources, the latency is higher at all mobilities for AODV-L. However, with very high PDF, this increase is expected. At high mobilities, the link breakages are very frequent and thus the local repairs (successful) increase the delay. In AODV, large number of packets are dropped due to the increased wait time. The unsuccessful route requests often do not account in the average delay because the packets are dropped and, hence, have less delay than AODV. However, at moderate mobilities, AODV has better average delay than AODV-L; at low mobilities, the delays are comparable for both the protocols.

However, the increased performances in the PDF and the AD are at the cost of the significant increase in routing load as shown in figure 5.13 and 5.14. It implies that at very high mobility, the local repairs are very frequent due to the link breakages and hence have very high routing load usually a factor of 3-5 in high packet rate traffic and of factor 3-7 in low packet rate traffic. The difference scales

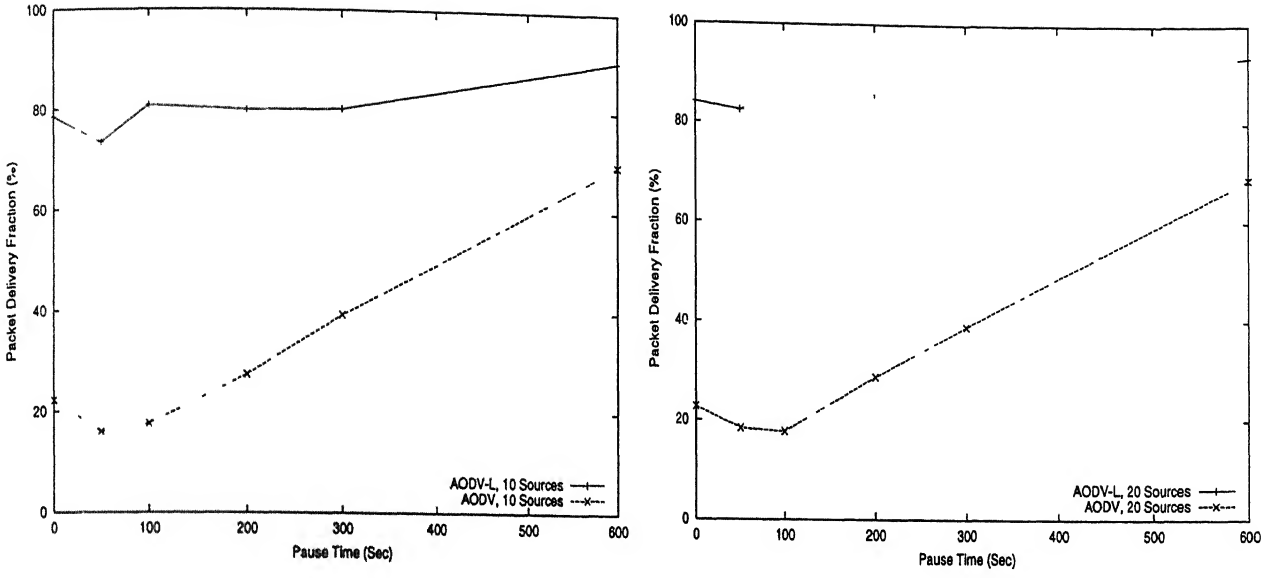


Figure 5.10: Packet Delivery Fraction in a Low Packet Network

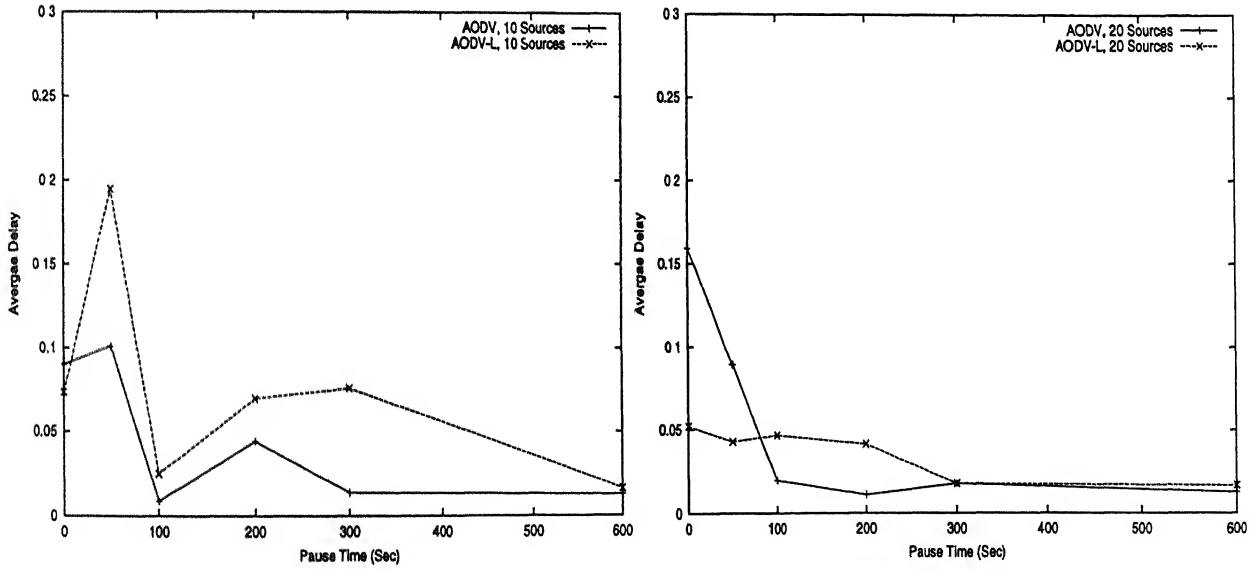


Figure 5.11: Average Delay in a 1 Packet/Sec Network

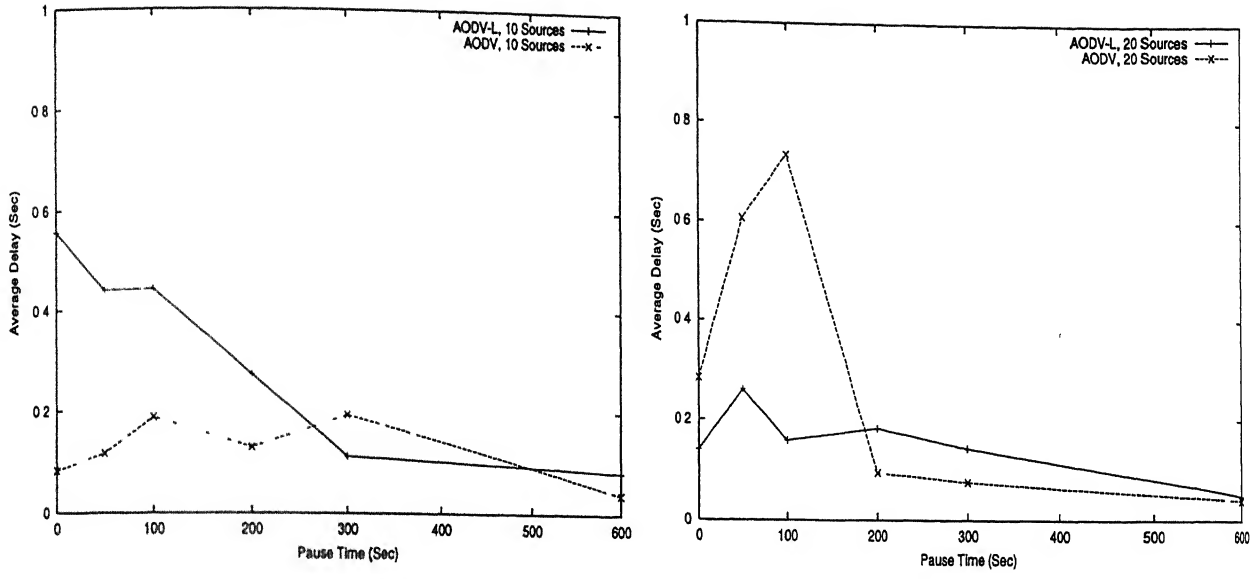


Figure 5.12: Average Delay in a Low Packet Network

down as the mobility decreases, and the number of sources increase. For example, in case of high packet traffic, the factor is of around 3 and in low packet traffic, it is of around 3-5. At very high mobilities, the link breaks are very frequent and multiple, each of it initiates the local repair. Hence, it results in increased routing load.

Since the PDF is very low in AODV, despite having low RL, for the reliable delivery of the packets, it requires many more retransmissions than it requires in AODV-L. Thus the gain offsets in terms of the overall efficiency.

5.2.4 Summary

The protocol presented, AODV-L, results in very good improvement in terms of PDF and AD. However, the aggressive local repair results in higher routing load. This routing load can be controlled with limited local repairs using counters at destinations.

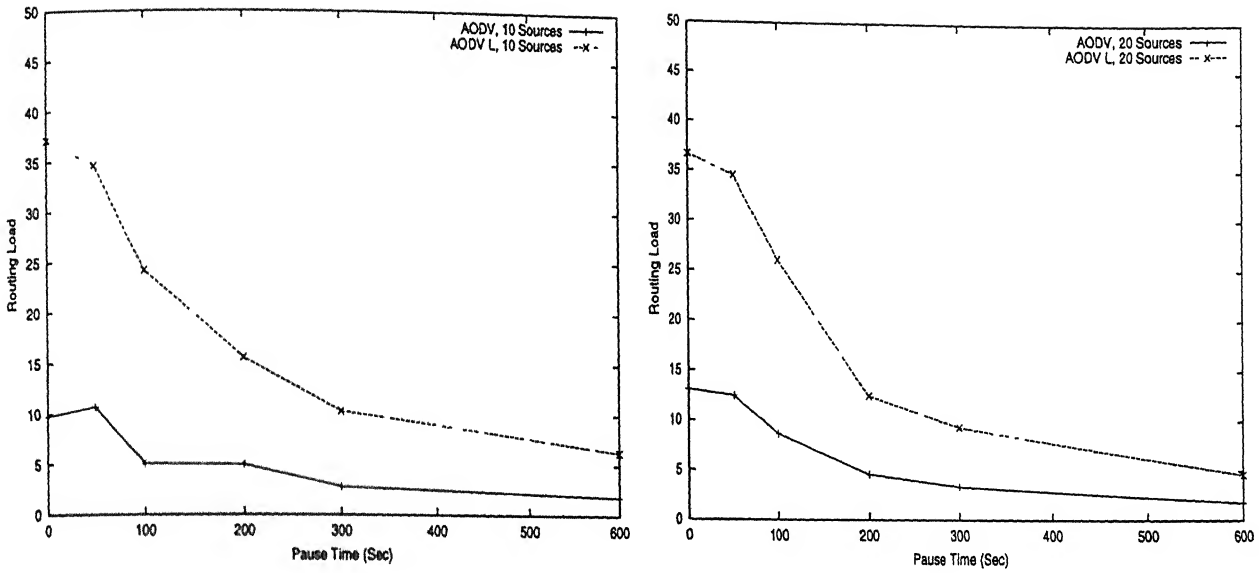


Figure 5.13: Routing Load in a 1 Packet/Sec Network

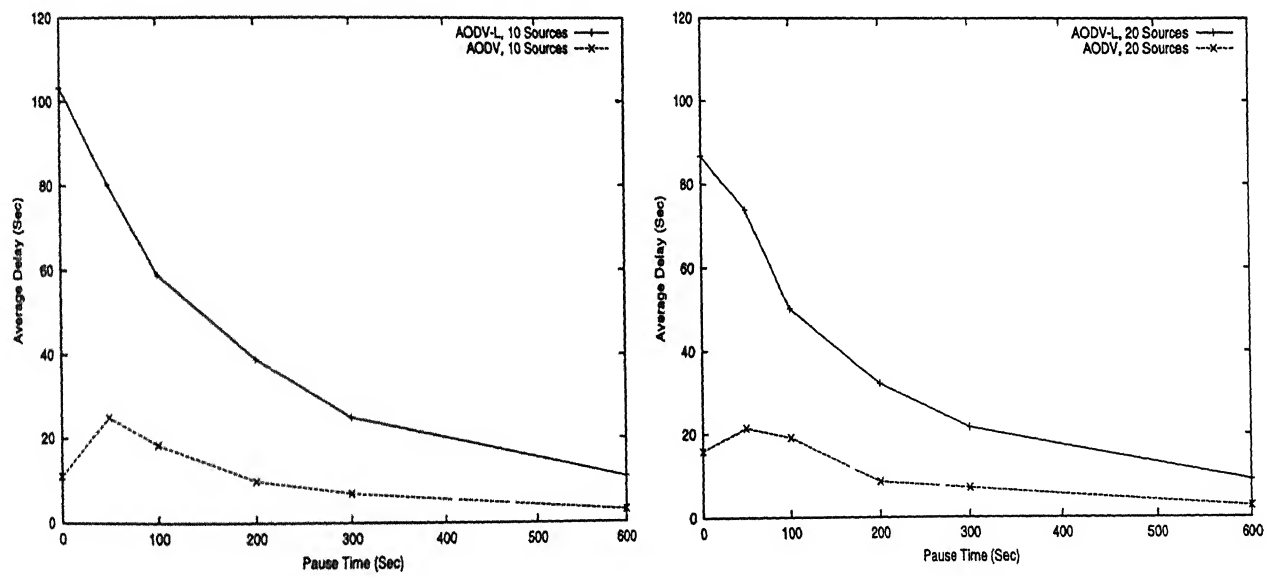


Figure 5.14: Routing Load in a Low Packet Network

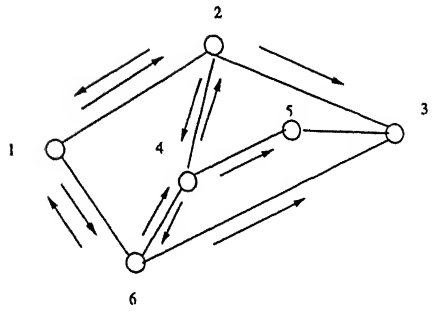


Figure 5.15: RREQ Packets Flow for a Destination

5.3 Alternate Paths and Quality of Service

In a highly mobile environment, if available, alternate paths may produce better results. AODV protocol results in only one path on a broadcast of a query. This approach is often found to be very much restrictive, particularly, in case of Quality Of Service (QoS) requirements. This section presents a scheme which provides alternate paths. The new scheme, may be easily adopted for the networks providing QoS.

With the increasing convergence of data networks and voice communications, the applications will demand QoS. The multimedia over the networks will depend on the ability of the network to provide the required QoS. The basic approach of the new scheme is similar to the AODV protocol. The route request/route reply cycle is used to find the path when it is required.

In the proposed scheme, we have taken care for the average case traffic requirements. A token based scheme is used which gets more than one path for the destination and can well be tried before the re-discovery cycle is initiated.

5.4 Effect of Multiple Replies in AODV

In AODV, for a route request, a route reply is sent. Other packets are ignored by the destination. Consider the case of the network shown in the figure 5.15. The node 1 wants to communicate with the node 3. The example figure shows the network state after the neighbors of the node 1, have broadcasted the query.

Let the RREQ packet reaches to the destination first through path $1-2-3$ and is replied back. In the original scheme, other packets, for example RREQ reaching the destination through path $1-6-3$, through $1-6-5-4-3$ or through $1-6-4-5-3$, are ignored. If a link fails on the path $1-2-3$, the path has to be rediscovered. In an ongoing connection, it may result in undesirable conditions. For example, the traffic demanding the less latency will suffer with such re-discoveries of the path. Consider the case of a protocol, when more than one paths are available for a single request. For example in the above network, if the path $1-6-3$ is also available, on a failure of the previous path, it can be used as an alternative path.

The protocol presented here, builds and utilizes such paths to stand as standy or alternative paths. It sent multiple replies on a single route request. In a network, where bidirectional links are available, multiple unicast replies will incur small overhead as against the complete path discoveries. The extra routing overhead will be dependent upon the number of hops in the path.

5.4.1 Protocol Description

The basic route discovery process is similar to the AODV route request/ route reply cycle. But instead of replying against a route requests only once, it replies *token* number of times. This *token* is decided on the QoS requirements of the application. Each node assigns a score *qosno* to the intermediate link being followed by the path. The function which assigns score may depend upon many parameters like the QoS requirements of the connection, buffer capacity at the link etc. This *qosno* is accumulated at the end of the path and sent back to the destination. Larger the *qosno* /hop_count ratio, better is the chance of the path being "good". Any intermediate node which does not satisfy the QoS requirements, drops the route request packets.

Multiple paths, thus, obtained can be used in two ways. If there is no requirements of the QoS, the extra path may serve as an alternative paths. On the other hand, if the source requires the QoS, it may be adapted to do so For example, in case of bandwidth requirements. The source may timeout wait for getting all the *tokens* replies and then based on the accumulated *qosno* may choose the better path.

In case of latency requirements, path can be selected either the order in which the replies are received or may decide on the accumulated *qosno*. The header contains a field which indicates whether the parameter of primary concern is bandwidth or delay. Accordingly, the path decision is taken. The link characteristics of neighbors can be learnt either using Hello messages or it can be obtained from the lower layers

The function which assigns scores are based on the requirements of the source. The source specifies the average case and the worst case requirements in the header extensions very much similar to one described in [Royer00]. Any node which does not satisfy the worst case requirements, drops the packet If the node satisfies the requirements, the node assigns a score on a fixed scale. Thus, finally it assembles the paths which at least satisfy the source requirements and have rough estimate about the average case behavior. The rest of the scheme is very much similar to the one described in the citation.

It uses extensions to the RREQ and RREP packets. The desired QoS parameters are specified in the extensions fields to the route requests packets. The intermediate node which receives the packet, checks whether it can provide the specified request or not. If it can, the packet is broadcasted further. On reaching the destination, the route reply, thus, generated will be able to satisfy the requirements. Routing tables include the entries like maximum delay, minimum bandwidth, average delay, average bandwidth, list of sources requesting delay guarantees and list of sources requesting bandwidth guarantees. An ICMP_QOS lost message is sent if any link is unable to satisfy the requirements sue to the change in the network.

5.4.2 Simulation Model

The simulation model is similar to the one described in the section 4.3. The connection pattern and the mobility models are the same as described in the section 4.3.1. The performance evaluation criteria also is same, that is, the packet delivery fraction, the routing load, and the average delay.

5.4.3 Performance Results

The protocol assumes two cases when (*i*) two replies are sent and (*ii*) three replies are sent. Figure 5.16 and figure 5 17 show the packet delivery Fraction (PDF) for high and low packet rate networks The packet delivery fraction is very much similar to the AODV and there is no significant improvement except in very large number of sources Thus, the multiple replies do not help in improving the packet delivery fraction.

- For less number of sources, the packet delivery fraction (PDF) at moderate to low mobilities, QODV shows slight improvements
- In moderate mobilities, for large number of sources, the gain is noticeable
-

Figure 5.18 and figure 5.19 show the routing load at high and at low packet rate traffic network.

- For QODV-2, the RL is comparably worse at high mobilities in high packet rate traffic.
- For less number of sources, multiple replies result in increased RL. When the number of sources are less, either it does not get multiple paths or even if it gets, the paths may have many links in common. Thus the breaks which occur are often common to both the paths and hence the path does not serve as an alternate path.
- As the number of sources increase or the mobility decreases, the RL is comparably better than AODV. The difference in pronounced in case of 40 sources specially at very high mobility and at low mobilities. In low packet rate traffic, however, it has better results for less number of sources.
- When the number of sources are large, the QODV-3 is better than QODV-2 while in less number of sources, QODV-2 is better than the QODV-3. When three paths are replied, it has more chances to get the path which have less

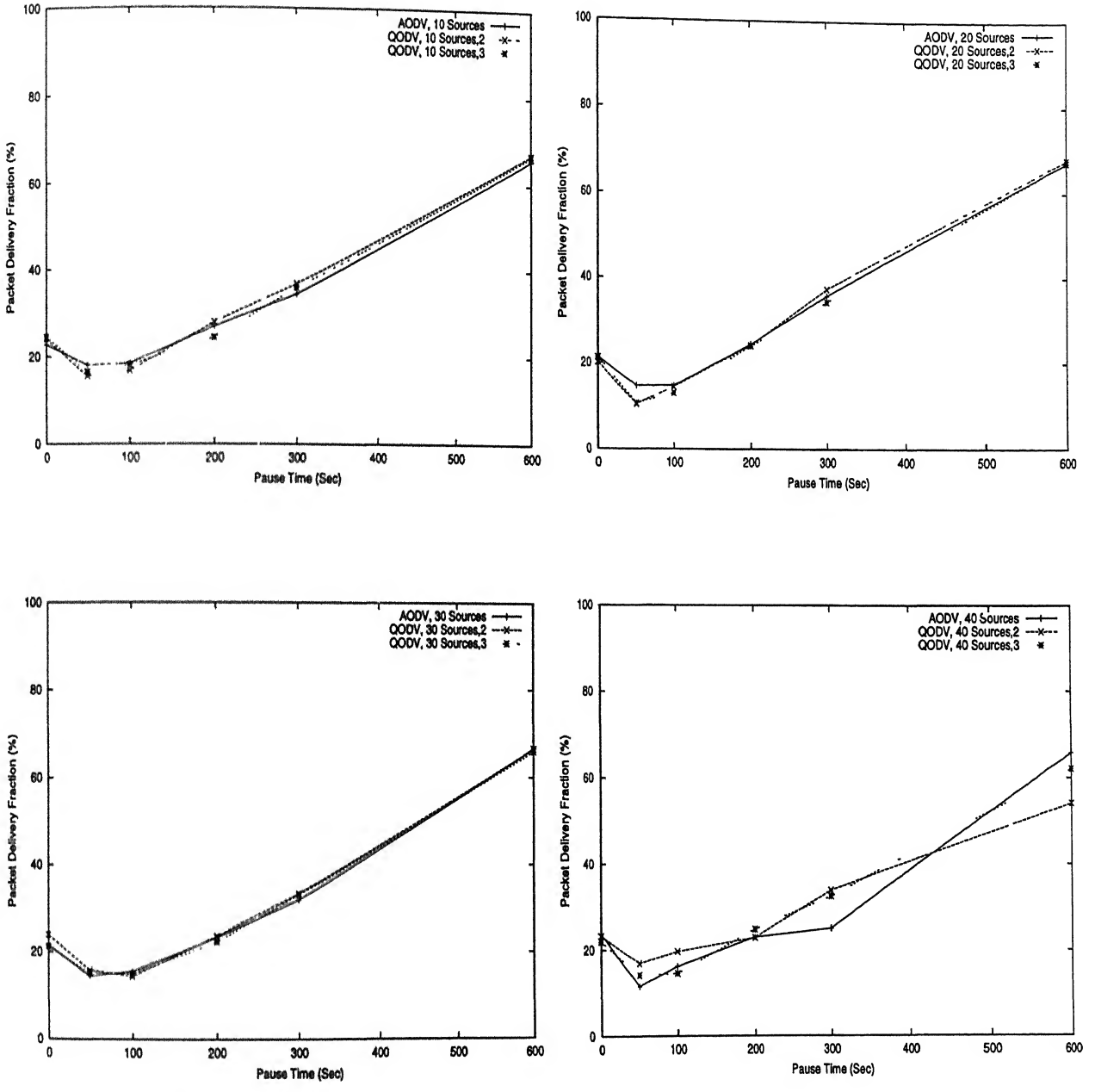


Figure 5.16: Packet Delivery Fraction at High Packet Rate

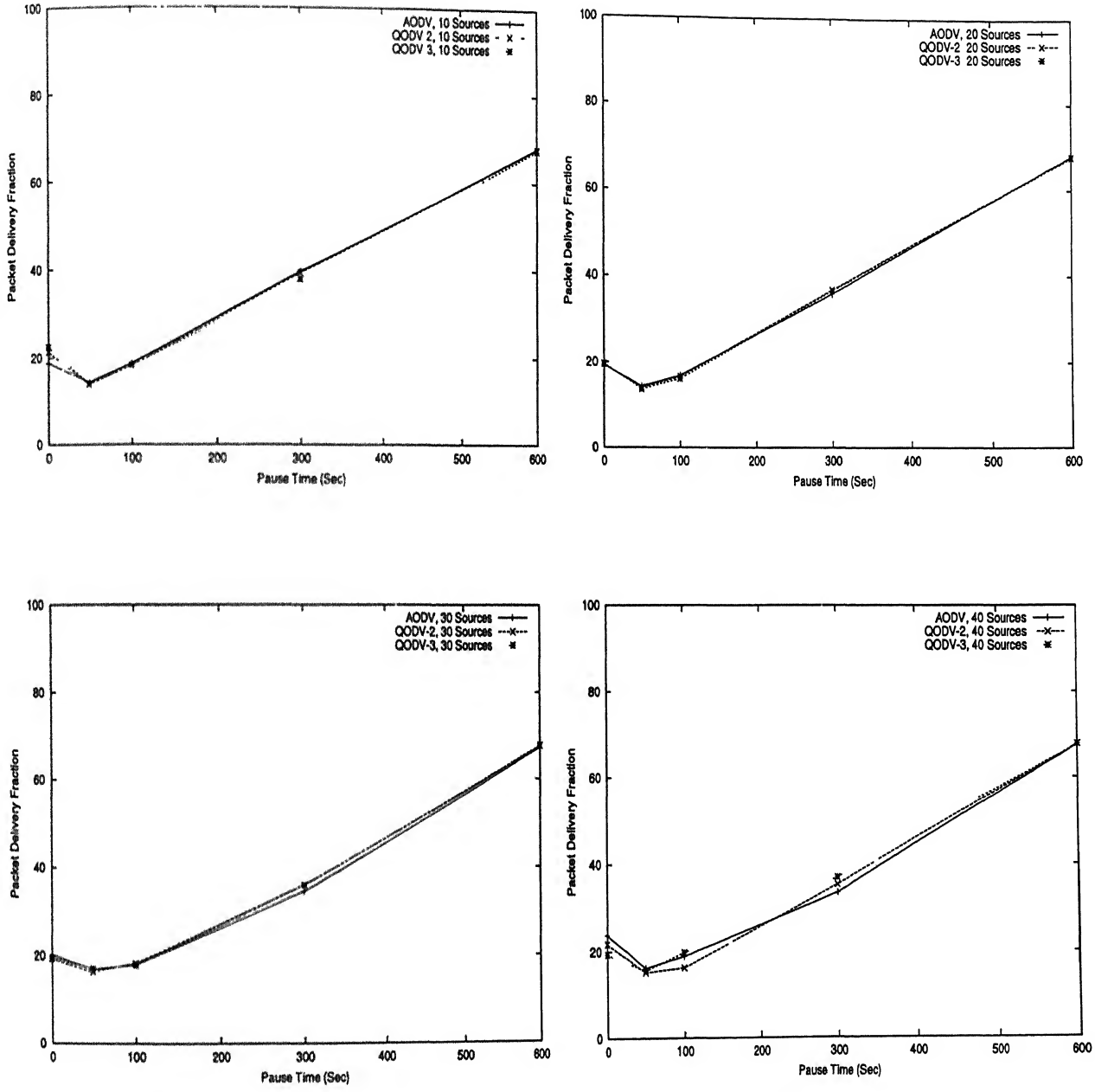


Figure 5.17: Packet Delivery Fraction at Low Packet Rate

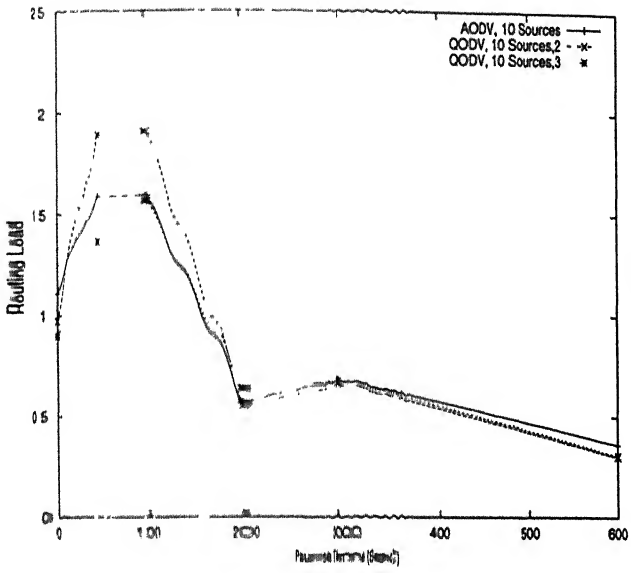
links in common. For 40 sources, the gain is of the factor 1-2. Very similar is its performance in low packet rate traffic

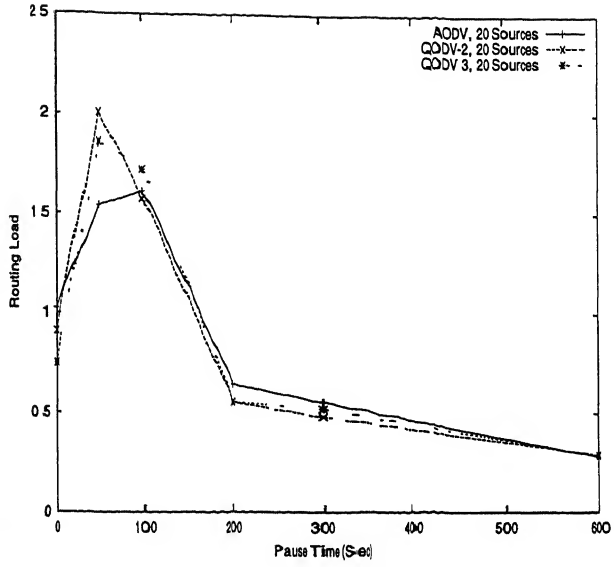
Figure 5.20 and 5.21 show the average delay at high and low traffic rate network.

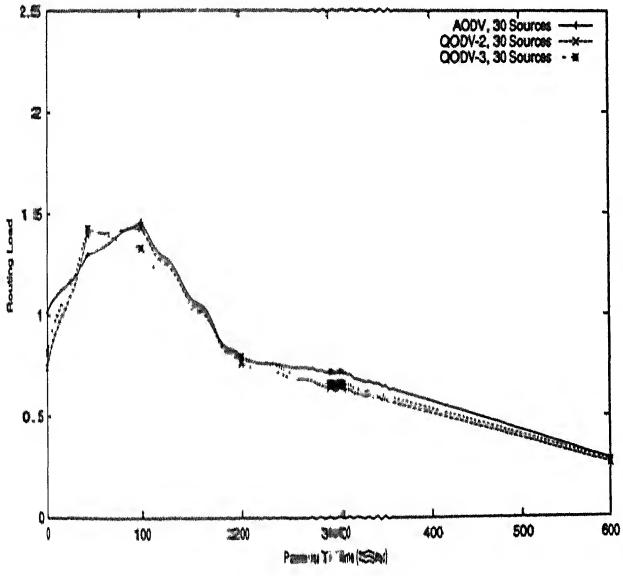
- In a low packet rate traffic, QODV-2 and QODV-3 both improve upon the average delay significantly. At less number of the sources, for around the same packet delivery fraction, it results in significantly improved delay
- At higher sources, however, the delay difference decreases. In high packet rate traffic, the delay is very much improved and remains consistent with mobilities.
- In high packet rate traffic, average delay is very sensitive and varies with mobilities significantly. QODV-3 performs better than QODV-2 for both the types of traffic.

5.4.4 Summary

In mobile environments, alternative paths are useful. The scheme presented scheme is able to take the advantage of multiple replies to serve them as alternative paths. When only two replies are sent, the scheme does not gains much, however in case of three replies it is evident that the scheme improves the performance of AODV protocol. For higher number of sources, the improvement is considerable.







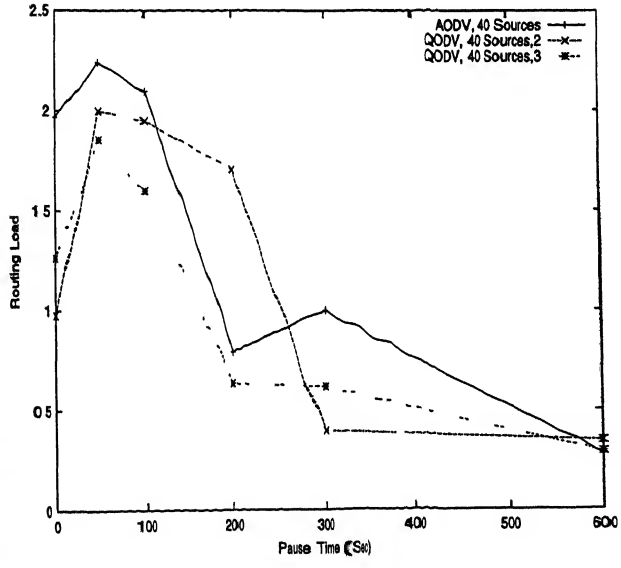


Figure 5.18: Routing Load at High Packet Rate

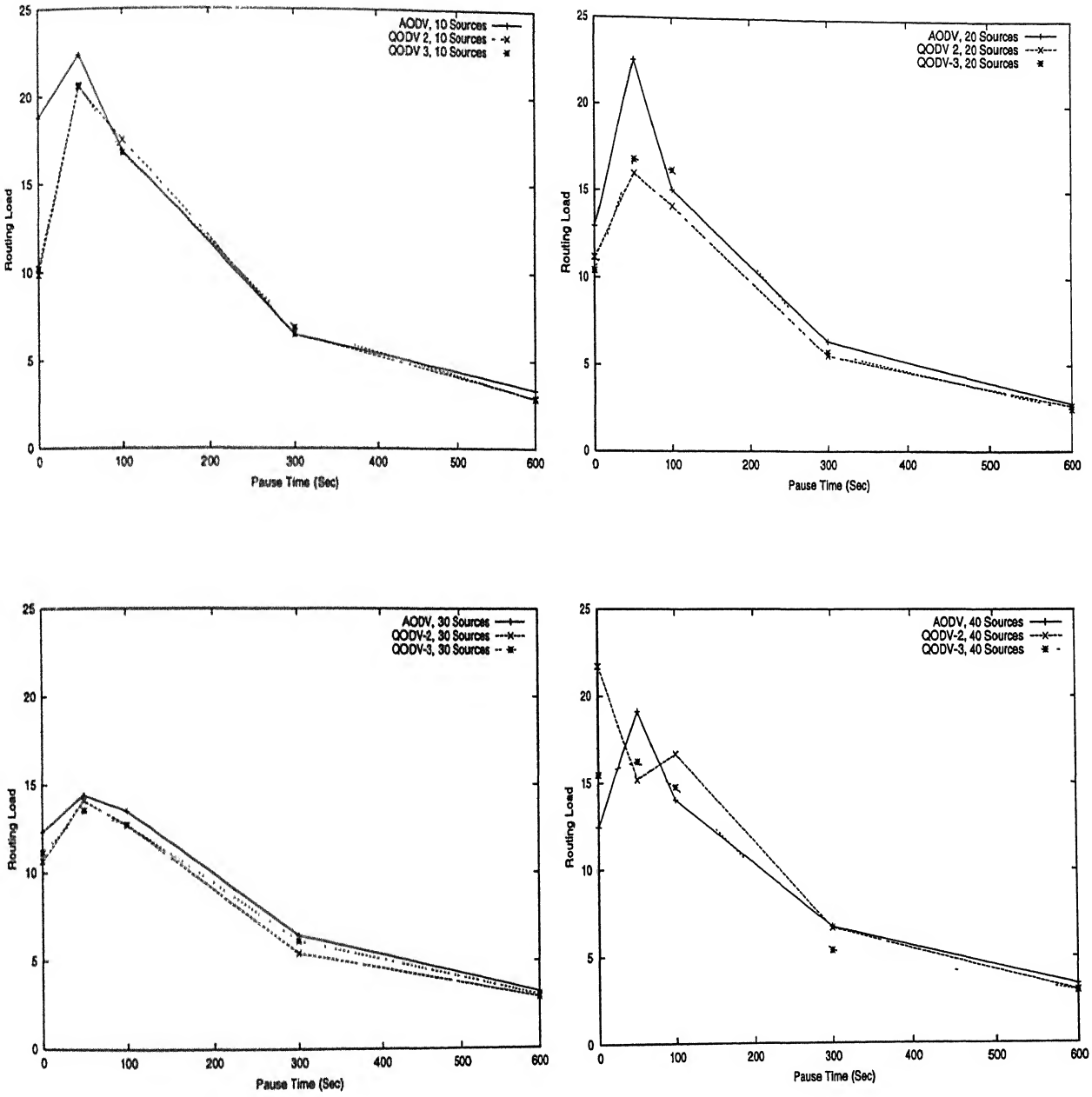
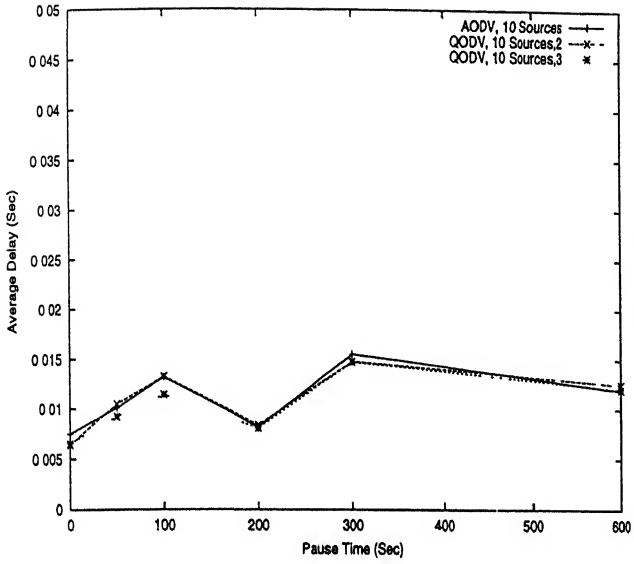
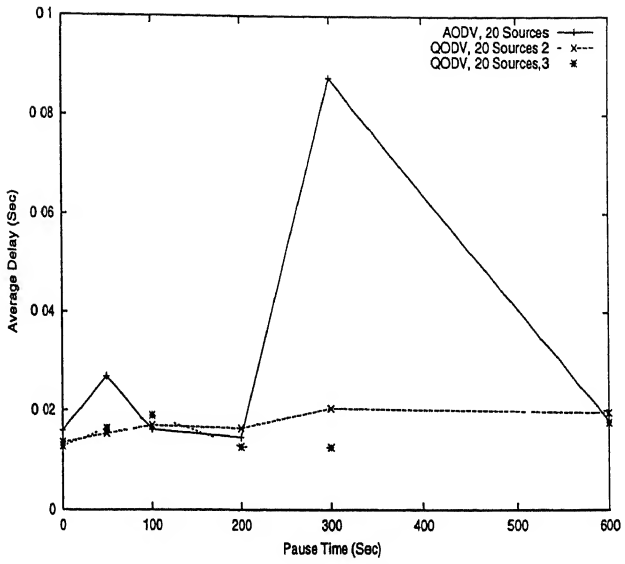
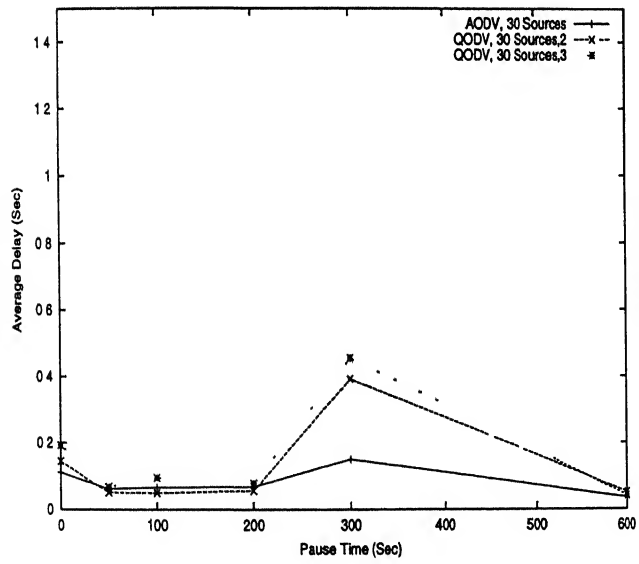


Figure 5.19: Routing Load at Low Packet Rate







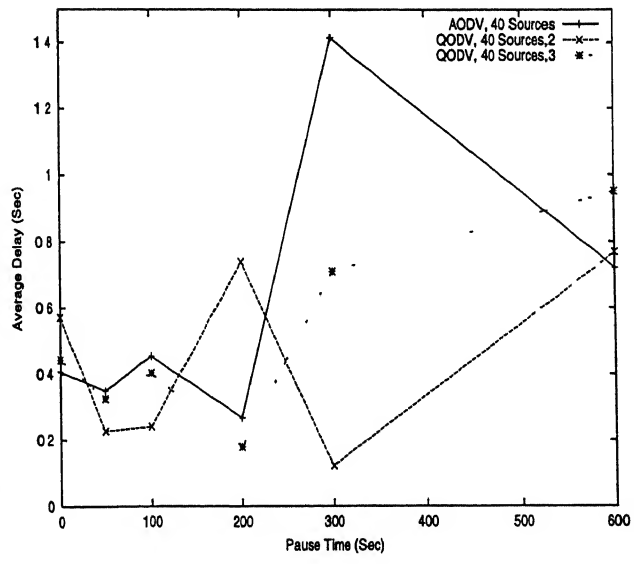


Figure 5.20: Average Delay at High Packet Rate

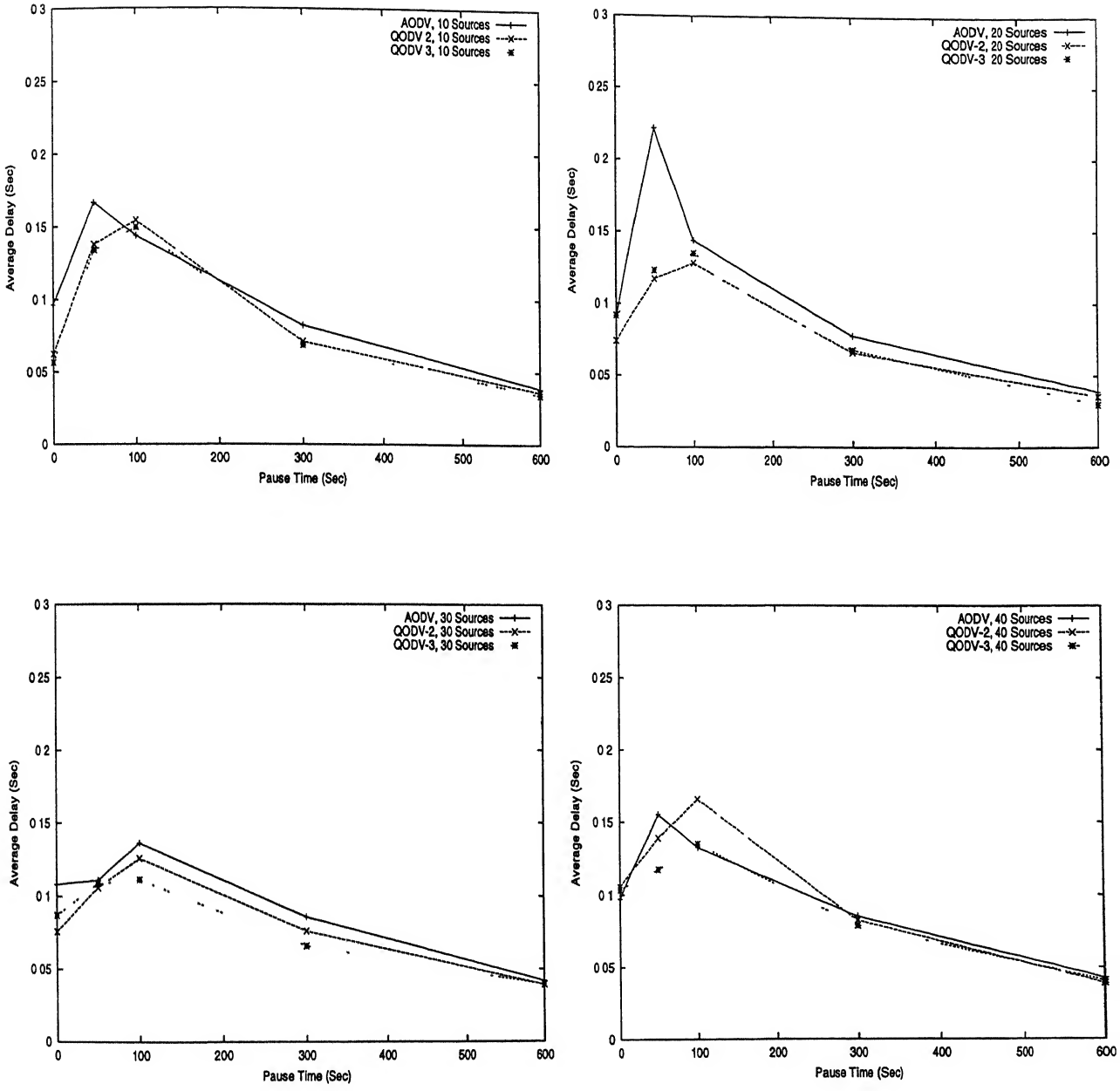


Figure 5.21: Average Delay at Low Packet Rate

Chapter 6

Conclusions and Future Work

MANETs consists of autonomous, self organizing and self operating nodes. MANETs are characterized to have links with less bandwidth, nodes with energy constraints, nodes with less memory and processing power and are more prone to security threats than the fixed networks. However, it has many advantages and its applications are different from the fixed networks, some of which are even not possible in the fixed networks. Routing is one of the main problems in MANETs Numerous solutions to routing have been proposed for such networks, but none of these solutions seem to satisfy the wide diversity of the wireless networks. AODV [Perkins99] is one of the protocol which takes care of many issues in establishing a route between a source and a destination when required. However, AODV is not able to satisfy many of the requirements.

The thesis explores the extensions and improvements of AODV. Chapter 1 of the report deals with a perceived visualization of transformations on the Internet usage pattern as increasingly more number of mobile users interact on it using wireless network connections. The chapter also discusses basic characteristics of a MANET, and focuses on the future applications as well as impediments in deployments of such networks.

Chapter 2 talks about the network routing problem in the general framework of graph theoretic problem. It presents the issues pertaining to restructuring and adaptations of basic routing schemes for wired networks to MANETs and how these

schemes have influenced design of routing protocols in MANETs. Performance of protocols are also discussed Chapter 3 gives a brief overview of some existing MANET routing protocols including AODV This chapter has been included mainly to provide a background of the direction of research in the area and the state-of-the-art

Chapter 4 studies the effects of the location information on AODV in establishing a route Two schemes using location information are presented which are differentiated by the location information is made available to the source The results show that these protocols can improve the performance of AODV considerably particularly in moderate and low mobilities. Thus, it is advantageous to use the scheme if location can either be tracked by the nodes or the can be obtained through GPS-like systems.

Chapter 5 deals with three different optimizations. One scheme uses source route caching at the nodes on the path The scheme shows a significant increase in packet delivery fraction. However, it results in increased routing load The scheme can be advantageous when there is less stress on bandwidth and the packet delivery is of primary concern.

The second scheme is based on the idea that the paths breaks are normally not high, in number, in a duration of an active connection In such cases, instead of complete path discovery, local repair scheme can be very much useful. The results show a large improvements in terms of packet delivery fraction. However, there is significant increase in routing load Keeping in view the number of retransmissions which AODV needs for reliable delivery of the packets, the routing load is not considered to be decidedly high. Thus, local repair can be used in the cases where, there is less constraint on bandwidth. The modifications can be made to limit the number of repairs to improve in other situations as well, particularly in high mobility.

Alternative paths, if available, can improve the performance in mobile environments The third scheme, extracts multiple paths without any extra route discovery cycle. The scheme results in significant gain in terms of average delay and routing load, particularly for large number of sources

The experiments have been carried out in a *ns-2* simulator which is an experimental network simulator widely available The core component is written in a object oriented language C++ and has OTcl/Tcl/Tk for interfacing

The protocols have been implemented with one modification to reflect the change due to the particular scheme Various combinations can be carried out to see the overall effect of all the schemes or some combinations of these schemes The local repair scheme with limited repairs can be carried out to find the best results depending upon the context A scheme based on the notions of the landmarks, which is expected to provide the scalability in the networks, combined with the local repair scheme presented, can be carried out to show the performance of the protocol. The scheme could not be implemented partly due to no support for implementation and testing of such schemes in *ns-2* and partly due to the time constraints.

Bibliography

[Bec00] Behcet Sarıkaya "Packet Mode ın Wireless Networks Overvıew of Transition to Third Generatıon" *IEEE Communıcatıons Magazıne* September 2000

[Bhag94] Charles E Perkıns and P. Bhagwat "Hıghly Dynamıc Destınation-Sequenced Dıstance-Vector Routing (DSDV) for Mobıle Computers" *Computer Communıcatıons Revıew* October 1994

[Broch98] J. Broch, D. A Maltz, D.B. Johnson, Y C. Hu and J. Jetcheva "A performance comparıson of multi-hop wireless ad hoc netwrok routing protocols " In *Proceedıngs of the 4th Internatıonal Conference on Mobıle Comutıng and Networkıng(MOBICOM'98)*, pages 85-97, October 1998.

[Chen98] T.-W Chen and M Gerla "Global State Routing. A New Routing Scheme for Ad-Hoc Wıreless Networks" In *Proceedıngs of IEEE International Conference on Computers and Communıcatıons* June 1998.

[Chi97] C.-C. Chiang, H.K. Wu, W.Liu, and M. Gerla "Routing in Clustered Mutihop, Mobile, Wıreless Networks with Fadıng Channels" In *Proceedıngs of IEEE SICON'97* pp 197-211, April 1997

[Chrıs00] Christopher Metz "IP over 2000·Where Have We Been and Where Are We Goıng?" *IEEE Internet Computıng* Jan/Feb 2000.

[Dube97] R. Dube, C.D. Rais, K.-Y. Wang and S.K. Tripathi "Signal Stability Based Adaptive Routing (SSA) for Ad-Hoc Mobile Networks *IEEE Personal Communications* Feb 1997

[Fall00] Kevin Fall and Kannan Vardhan "*ns*-notes and documentation, 2000 available from *http://www.isi.edu/nsnam/ns*"

[Gerla98] C.R. Liu and M Gerla "MACA/PR An Asynchronous Multimedia Mutihop Wireless NEtwork" In *Proceedings of IEEE INFOCOM'97* March 1997.

[Grace00] K Grace "Mobile Mesh Routing Protocol","Mobile Mesh Border Discovery Protocol", and "Mobile Mesh Link Discovery Protocol" available at *http://search.ietf org/internet-drafts/draft-grace-manet-mm*-00.txt*

[Haas01] Zygmunt J. Haas, Marc R Pearlman, and Prince Samar "The Intrazone Routing Protocol (IARP) for Ad Hoc Networks" and "The Interzone Routing Protocol (IERP) for Ad Hoc Networks" *Internet Draft* available at *http://search ietf org/internet-drafts/draft-ietf-manet-zone-iarp-00.txt* and *http://search ietf.org/internet-drafts/draft-ietf-manet-zone-ierp-00 txt*, Work In Progress, Jan 2001.

[Hong00] Mario Gerla, Xiaoyan Hong and Guangyu Pei "Landmark Routing Protocol (LANMAR) for Large Scale Ad Hoc Networks" *Internet Draft* available at *http://search.ietf.org/internet-drafts/draft-ietf-manet-lanmar-00.txt* Work In Progress, Dec. 2000

[IETF47] Charles E. Perkins "Mobile Networking at IETF 47" *Mobile Computing and Mobile Communications Review"* Winter 2000

[Imei96] Tomasz Imielinski and Julio C. Navas " Geographic Addressing, Routing, and Resource Discovery with the Global Positioning System."

[Iwata99] Atsushi Iwata, Ching-Chuan Chiang, Guangyu Pei, Mario Gerla and Tsu-wei Chen "Scalable Routing Strategies for Ad hoc Wireless Networks" PhD dissertation.

[Johan99] Per Johansson, T. Larsson, N. Hedman and B Mielczarel. "Routing protocols for mobile ad hoc networks - a comparative performance analysis " *Proceedings of the 5th International Conference on Mobile Computing and Networking(MOBICOM'99)*

[Jac01] P Jacquet, P. Muhlethaler, A Qayyum, A Laouiti, L Viennot, and T Clausen "Optimized Link State Routing Protocol" *Internet Draft* available at *http·//search ietf org/internet-drafts/draft-ietf-manet-olsr-04.txt* Work In Progress, March 2001

[John96] D B Johnson and D.A Maltz "Dynamic Source Routing in AD-Hoc Wireless Networks" In "*Mobile Computing*" ed T. Imielinski and H Korth, KAP, 1996

[John97] John Scourias " Overview of the Global System for Mobile Communication" a tutorial on GSM

[Monarch98] *ns-2* wireless extension document available at *ftp.//ftp monarch.cs cmu edu/pub/monarch/wireless/wireless-sim/ns-cmu.ps*

[Navid01] : Navid.Nikaein "Distributed Dynamic Routing Algorithm" available at *http://www.eurecom fr/ nikaeinn/ddr.pdf*

[Nitin98] Young-Bae Ko and Nitin H. Vaidya "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks." In *Proceedings of the 4th International Conference on Mobile Comuting and Networking(MOBICOM'98)*, October 1998.

[Park97] V.D. Park and M.S. Corson "A highly Adaptive Distributed Routing Algorithm fro Mobile Wireless Networks" In *Proceedings of IEEE INFOCOM'97* April 1997.

[Pei00] Mario Gerla, Guangyu Pei, Xiaoyan Hong and Tsu-Wei Chen "Fisheye State Routing Protocol (FSR) for Ad Hoc Networks" *Internet Draft*

available at *http://search ietf org/internet-drafts/draft-ietf-manet-fsr-00 txt* Work In Progress, Dec 2000.

[Perkins97] Charles E Perkins "Mobile Networking Thorugh Mobile IP" a tutorial available at *http //www computer org/internet/v2n1/perkins htm"*

[Perkins00] Samir R Das, Charles E Perkins and E M Royer "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks" In *Proceedings of the 1st Conference on Computer Communications(INFOCOM'00)*

[Perkins99] Charles E Perkins and E M. Royer "Ad Hoc On Demand Distance Vector Routing" In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pages 90-100, Feb 1999

[rfc2501] "Mobile Ad Hoc Networking Routing Protocol Performance Issues and Evaluation Considerations " Request For Comments 2501 available at *http://www.ietf.org*

[Royer01] Samir R Das, Charles E Perkins and E M. Royer "Ad Hoc On Demand Distance Vector Routing" IETF Internet Draft (Work In Progress) *http //www.ietf.org/internet-drafts/draft-ietf-manet-aodv-08.txt* March 2001

[Sinha99] P. Sinha, R. Sivakumar and V. Bhargavan "CEDAR· a Core Extraction Distributed Ad Hoc Routing Algorithm" In *Proceedings of IEEE INFOCOM'99* March 1999

[Tay99] Jiang Mingliang, Li Jinyang and Y.C Tay "Cluster Based Routing Protocol" old *Internet Draft* available at *http://www.ietf.cnri.reston va.us/proceedings/98dec/slides/manet-cbrp-98dec/* Jan 1999.

[Toh97] C.-K Toh "Associativity-Based Routing for Ad-Hoc Mobile Networks" *Wireless Personal Communications* Vol. 4, No 2, March 1997

134258

Date Slip

The book is to be returned on the date last stamped.

.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....